Lignes directrices sur la protection des données pour le traitement des données à caractère personnel à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme

Comité de la Convention
pour la protection des personnes
à l'égard du traitement automatisé
des données à caractère personnel

Règles et principes
de protection des données

Convention 108

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Lignes directrices sur la protection des données pour le traitement des données à caractère personnel à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme

Adoptées par le Comité de la Convention
pour la protection des personnes
à l'égard du traitement automatisé
des données à caractère personnel
(Convention 108)

Conseil de l'Europe

Édition anglaise :
Guidelines on data protection for the processing of personal data for anti-money laundering/countering the financing of terrorism purposes

Conception de la couverture et mise en page : Service de la production des documents et des publications (SPDP), Conseil de l'Europe

Photo : Shutterstock.

Imprimé dans les ateliers du Conseil de l'Europe

Table des matières

Abréviations/acronymes

BC/FT : blanchiment de capitaux / financement du terrorisme

BE : bénéficiaire effectif

CADH : Convention américaine des droits de l'homme

CADHP : Charte africaine des droits de l'homme et des peuples

CEDH : Convention européenne des droits de l'homme

CJUE : Cour de justice de l'Union européenne

CRF : cellules de renseignement financier

DOS : déclaration d'opération suspecte

DUDH : Déclaration universelle des droits de l'homme

EPNFD : entreprises et professions non financières désignées

EA : entité assujettie

GAFI : Groupe d'action financière

IA : intelligence artificielle

IF : institutions financières

LBC/FT : lutte contre le blanchiment de capitaux / financement du terrorisme

MONEYVAL : Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme

PIDCP : Pacte international des droits civils et politiques

PPE : personnes politiquement exposées

PPP : partenariat public-privé

PSAV : prestataires de services d'actifs virtuels

1. Introduction

1.1. Généralités

Le blanchiment de capitaux et le financement du terrorisme (BC/FT) sont des phénomènes criminels impliquant fréquemment des stratagèmes transfrontières et l'utilisation abusive d'institutions et d'entités financières et non financières situées dans plusieurs juridictions. Le partage de données entre acteurs étatiques et non étatiques est donc crucial pour lutter efficacement contre ces phénomènes criminels. Le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT[1]) poursuit à la fois des buts de prévention, d'investigation et de poursuites, à travers un système de mesures mises en œuvre par de multiples acteurs : en particulier les entités soumises à obligation de déclaration (entités assujetties - EA) et leurs clients, les cellules de renseignement financier (CRF), les services répressifs et de supervision, les autorités chargées des poursuites, les systèmes judiciaires, les douanes et les responsables politiques à différents niveaux.

Les politiques de LBC/FT comprennent un traitement et un partage de données pertinents qui doivent être effectués dans le plein respect des cadres applicables en matière de protection des données, en particulier la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (STE n° 108), telle que modifiée par le Protocole STCE n° 223 (« Convention 108+ »), comme illustré dans les sections suivantes.

Le traitement des données à caractère personnel à ces fins peut constituer une ingérence dans le droit de la personne concernée au respect de la vie privée, tel que protégé par l'article 8 de la Convention européenne des droits de l'homme (STE n° 5, la «Convention») et d'autres instruments internationaux relatifs aux droits de l'homme (notamment l'article 12 de la Déclaration universelle des droits de l'homme (DUDH), l'article 17 du Pacte international des

1. Normes du Conseil de l'Europe : Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE n° 198). Pour ce document, les articles suivants de la Convention STCE n° 198 sont d'importance particulière : articles 7, 17, 18, 19, 20, 43, 46, 47. Normes universelles en matière de BC/FT : normes du GAFI.

droits civils et politiques (PIDCP), l'article 11.2 de la Convention américaine des droits de l'homme (CADH), et l'article 4 de la Charte africaine des droits de l'homme et des peuples (CADHP). Selon la jurisprudence, la vie privée d'un individu doit être interprétée au sens large, y compris les informations relevant à la fois de sa sphère privée et de sa vie professionnelle ou publique. En vertu de l'article 2.*a* de la Convention 108+, tout type d'information peut être une donnée à caractère personnel s'il se rapporte à une personne identifiée ou identifiable, qui pourrait être une information relative à la vie privée d'une personne, ce qui inclut également les activités professionnelles, ainsi que des informations publiques sur sa vie. En vertu de l'article 11 de la Convention 108 modernisée, les exceptions et restrictions à ce droit ne sont admises que si elles poursuivent un objectif légitime d'intérêt public et (i) sont prévues par la loi ; (ii) respectent l'essence des droits et libertés fondamentales; et (iii) constituent une mesure nécessaire et proportionnée dans une société démocratique pour atteindre ce but légitime.

Le régime de LBC/FT prévoit plusieurs contextes de traitement des données à caractère personnel, qui sont essentiellement fondés sur l'intérêt public, en définissant des obligations détaillées pour les responsables du traitement. Cela s'étend au traitement des données à caractère personnel par les autorités gouvernementales qui sont habilitées par la loi à lutter contre la LBC/FT et qui sont dotées de pouvoirs spécifiques dans ce domaine. Néanmoins, il n'en va pas de même pour les institutions du secteur privé, qui sont des entités assujetties, qui n'ont pas le même statut juridique ni le même mandat. Dans le même temps, leur rôle et leurs obligations concrètes en tant que gardiens pour prévenir l'utilisation abusive du système financier à des fins de BC/FT doivent également être dûment reconnus. Cependant, le traitement des données par les entités du secteur privé sur la base légale de l'intérêt public doit être envisagé avec prudence et seulement lorsqu'une base légale claire autorisant ce traitement existe, notamment dans le contexte des nouvelles initiatives de mise en commun de données qui impliquent le partage des données entre les entités du secteur privé (qui ne font pas partie du même groupe financier).

En tout état de cause, l'intérêt public doit être spécifiquement défini et limité aux circonstances dans lesquelles les mesures bénéficient et augmentent l'efficacité du régime de LBC/FT. Cela implique, par exemple, que la collecte et le traitement excessifs de données à caractère personnel soient évités parce que cela n'est pas conforme aux principes de protection des données. En outre, une collecte excessive de données ne sert pas toujours les objectifs opérationnels et les finalités prévues par la loi, et risque aussi de créer des difficultés juridiques et techniques supplémentaires (qualité/mise à jour des données, sécurité des données, etc.) pour les principales parties prenantes, y compris les services répressifs.

L'évolution récente a également mis en évidence un besoin de clarifications additionnelles dans des domaines importants tels que l'accès du grand public à l'information sur la propriété effective[2], qui a été considérée comme constituant une ingérence grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel[3], car cela rend publique une grande quantité de données à caractère personnel sur les bénéficiaires effectifs dans un pays. Ce cas montre que ce domaine est en constante évolution et que de plus en plus de réglementations, y compris de droits contraignants, mais aussi d'autres jurisprudences dans ce domaine sont attendues dans un proche avenir.

Étant donné que la protection des données est fondamentale pour garantir le droit au respect de la vie privée, de la vie familiale, de la correspondance et du domicile (article 8 de la Convention), il convient de tenir compte des règles et principes qui l'encadrent lorsque l'on agit dans l'intérêt de la lutte contre le blanchiment de capitaux et le financement du terrorisme, conformément aux engagements et obligations des États parties découlant du droit international. En vertu de la législation, l'existence d'un objectif légitime, d'une base juridique valable et de garanties appropriées pour le traitement des données à caractère personnel est une condition préalable, pour laquelle la logique sous-jacente doit être soigneusement analysée et énoncée par les principaux acteurs des domaines de la LBC/FT, de la protection des données et des droits humains. Compte tenu du fait que le traitement et le partage des données jouent un rôle crucial dans la LBC/FT, ces lignes directrices[4] visent à mettre l'accent sur les exigences prévues par la Convention 108+ pour les responsables du traitement et les sous-traitants, tout en se conformant au cadre de la LBC/FT.

1.2. Champ d'application

L'objectif de ces lignes directrices est de fournir des orientations sur la manière d'intégrer les exigences de la Convention 108+ dans le domaine de la LBC/FT afin d'assurer un niveau approprié de protection des données tout en facilitant les flux transfrontières de données, et de mettre en évidence certains domaines dans le contexte de la LBC/FT dans lesquels des garanties en matière de protection des données devraient être renforcées.

2. Voir la définition de « l'information sur les bénéficiaires effectifs » en annexe.
3. Arrêt de la Cour de justice de l'Union européenne (CJUE) du 22 novembre 2022 dans les affaires jointes C-37/20 Luxembourg Businesses Registers et C-601/20 Sovim.
4. Les lignes directrices ont été élaborées en tenant compte des contributions de plusieurs membres, d'experts et du secrétariat du Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme (MONEYVAL).

Ces lignes directrices visent également à fournir aux gouvernements et aux décideurs des recommandations de base qui devraient être prises en compte dans la conception de politiques et d'instruments réglementaires conformes aux normes internationales de protection des données et de la vie privée, prévues par la Convention 108+.

2. Définitions et terminologie

Les définitions proposées dans cette partie sont jugées nécessaires à une bonne compréhension du contexte de la lutte contre le blanchiment de capitaux et le financement du terrorisme. En outre, d'autres définitions spécifiques à ce domaine figurent en notes de bas de page et dans les chapitres correspondants.

Données à caractère personnel et personne concernée – L'article 2.*a* de la Convention 108+ définit les données à caractère personnel comme toute information relative à une personne physique identifiée ou identifiable (personne concernée). Une personne est considérée comme identifiable lorsqu'il est possible d'obtenir, sans délais ni efforts déraisonnables, des compléments d'information qui peuvent permettre à terme d'identifier directement ou indirectement la personne concernée. Dans le contexte de la LBC/FT, les clients, les bénéficiaires effectifs[5], les parties aux virements électroniques ou les personnes dont les informations identifiables sont contenues dans les transferts de données doivent être considérés comme des personnes concernées. Ils sont les principaux sujets des mesures de vigilance à l'égard de la clientèle (CDD)[6], y compris l'identification et la vérification de l'identité. Alors que la Convention 108+ protège principalement les données à caractère personnel des personnes physiques, les Parties peuvent étendre la protection dans leur

5. Selon la définition du GAFI, un bénéficiaire effectif est la ou les personnes physiques qui possèdent ou contrôlent en dernier ressort un client, et/ou la personne physique pour le compte de laquelle une transaction est effectuée. Cela inclut également les personnes qui exercent un contrôle effectif ultime sur une personne morale ou une construction juridique.
6. La vigilance à l'égard de la clientèle est un processus dans lequel les informations pertinentes sur le client d'une entité obligée sont collectées et évaluées du point de vue du BC/FT. Les entités soumises à l'obligation de déclaration doivent avoir mis en place des procédures pour identifier et éventuellement signaler les risques de blanchiment et de financement du terrorisme associés à une relation d'affaires ou à une transaction occasionnelle. Les recommandations 10, 11, 12, 15 et 17 du GAFI détaillent les mesures de vigilance à l'égard de la clientèle de base et supplémentaires que doivent adopter les institutions financières. La recommandation 22 étend ces mesures aux entreprises et professions non financières désignées (EPNFD).

droit national aux données relatives aux personnes morales et constructions juridiques afin de protéger leurs intérêts légitimes[7], bien que les données d'entreprises ne soient pas à considérer comme des données à caractère personnel, à moins qu'elles ne concernent une personne physique (sociétés unipersonnelles ou données relatives aux clients, par exemple).

Traitement des données – Toutes les opérations effectuées sur des données à caractère personnel aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme, qu'elles soient automatisées ou manuelles, peuvent être définies comme des traitements de données – y compris la collecte, le stockage, la conservation, la modification, l'extraction, la divulgation, la mise à disposition, l'effacement, l'utilisation, la destruction et la réalisation d'opérations logiques et/ou arithmétiques sur ces données (article 2, points *b* et *c*, de la Convention 108+). Les opérations susmentionnées ne sont effectuées que lorsque les responsables du traitement et, le cas échéant, les sous-traitants prennent toutes les mesures appropriées (et démontrables) pour se conformer aux dispositions de la Convention 108+ (article 10, paragraphe 1).

Responsables du traitement des données (en LBC/FT) – Une personne physique ou morale ou une construction juridique[8], une autorité publique, un service, une agence ou toute autre entité qui, seule ou conjointement avec d'autres, dispose du pouvoir de décision en ce qui concerne le traitement des données, la finalité et les moyens du traitement, ainsi que les catégories de données à traiter et l'accès aux données (article 2.*d* de la Convention 108+). Le pouvoir de décision peut découler d'une désignation légale ou de circonstances factuelles à apprécier au cas par cas[9]. Les responsables du traitement sont tenus de garantir la légitimité du traitement des données (article 5 de la Convention 108+).

Dans le contexte de la LBC/FT, les entités assujetties sont soit seules, soit coresponsables du traitement. Ces mêmes entités assujetties peuvent être des institutions financières (IF[10]), des entreprises et professions non financières

7. Rapport explicatif de la Convention 108+, paragraphe 30.
8. Alors que la Convention 108+ fait référence aux « personnes morales » dans son article 2, les Normes du GAFI établissent une distinction entre les personnes morales et les constructions juridiques. Pour plus de détails, veuillez consulter l'annexe.
9. Rapport explicatif de la Convention 108+, paragraphe 22.
10. La notion d'« Institution financière (IF) » dans le domaine de la LBC/FT, telle qu'elle est utilisée dans les présentes lignes directrices, comprend à la fois les établissements de crédit et les institutions financières.

désignées[11] (EPNFD) ou des prestataires de services d'actifs virtuels (PSAV). Les destinataires des informations, notamment les cellules de renseignement financier (CRF), les autorités répressives ou d'autres entités, y compris celles qui gèrent les registres publics d'informations sur les propriétaires de base et les bénéficiaires effectifs, doivent être considérés comme des responsables du traitement de données pour le traitement des données à caractère personnel qu'ils effectuent.

Le cadre de la LBC/FT peut prévoir différentes situations de partage d'informations, notamment entre les entités assujetties, entre les personnes morales ou constructions juridiques et les contrôleurs des registres de propriété effective, entre les entités assujetties et les cellules de renseignement financier (CRF) ou entre les entités assujetties et une autre autorité compétente (« partenariats public-privé/PPP »), entre les CRF, les services répressifs et de supervision et les autorités judiciaires de différents pays, et entre les CRF et d'autres autorités compétentes. Dans ces cas, lorsque les différents responsables du traitement ont le pouvoir de décider des aspects pertinents des opérations de traitement concernant les mêmes données à caractère personnel, telles que le but dans lequel la donnée à caractère personnel est traitée, ils doivent être considérés comme des responsables conjoints du traitement[12]. Ce statut conjoint entraîne la responsabilité conjointe d'une activité de traitement. Afin de répondre à des réalités de traitement des données de plus en plus complexes, le traitement conjoint peut prendre diverses formes et la participation des différents responsables du traitement peut être inégale. Par conséquent, ces derniers doivent déterminer leurs responsabilités respectives en ce qui concerne le respect des obligations prévues par le règlement d'un accord spécifique.

Sous-traitants des données (en LBC/FT) – Un sous-traitant est la personne physique ou morale ou la construction juridique qui traite des données à caractère personnel pour le compte d'un responsable du traitement. Les activités confiées à un sous-traitant peuvent être limitées à une tâche très spécifique ou, au contraire, être assez générales. Les personnes physiques ou morales appliquant des mesures de vigilance au nom d'institutions financières (IF) et d'autres entreprises et professions non financières désignées ne sont réputées sous-traitantes des données que dans le cas où elles ne font que suivre les

11. Par exemple les casinos, agents immobiliers, négociants en métaux précieux et pierres précieuses, avocats, notaires, autres professionnels du droit indépendants, ainsi que les comptables (lorsqu'ils agissent à titre d'avocats exerçant seuls, d'associés ou de professionnels salariés au sein de cabinets professionnels) et les prestataires de services aux sociétés et fiducies (pour la fourniture de certains services). Toutefois, certains secteurs ne sont pas toujours couverts de façon appropriée (par exemple les avocats et les comptables internes).
12. Conformément au paragraphe 22 du rapport explicatif de la Convention 108+ (coresponsable d'un traitement et éventuellement responsable de différents aspects de ce traitement).

instructions données par les responsables. La principale différence avec les responsables du traitement des données réside dans le pouvoir de décision en ce qui concerne le traitement des données en question (dans le domaine de la lutte contre le blanchiment de capitaux et le financement du terrorisme, pour se conformer aux mesures de vigilance à l'égard de la clientèle). Toutefois, les sous-traitants peuvent également devenir des responsables du traitement lorsque le traitement des données est effectué à leurs propres fins ou lorsque les conditions de traitement des données prescrites par les responsables du traitement sont violées.

Catégories particulières de données à caractère personnel (données sensibles) – Dans l'article 6, il existe des catégories particulières de données à caractère personnel dont le traitement est, par nature, susceptible de présenter un risque plus élevé pour les personnes concernées. Leur traitement nécessite donc d'autres garanties complétant celles déjà en place pour les catégories de données à caractère personnel en général. Les catégories ci-après de données à caractère personnel considérées comme sensibles sont celles qui révèlent : (i) des origines raciales ou ethniques ; (ii) des opinions politiques, des convictions religieuses ou autres, y compris les convictions philosophiques ; (iii) une appartenance syndicale ; (iv) des données génétiques ; (v) des données biométriques traitées dans le but d'identifier une personne de manière unique ; (vi) de l'état de santé ; (vii) la vie sexuelle ou l'orientation sexuelle ; (viii) des infractions, procédures pénales, condamnations et mesures de sécurité connexes.

3. Principes de base pour la protection des données à caractère personnel

3.1. Le principe de la limitation de la finalité

Principe général

Le traitement des données à caractère personnel doit être effectué pour des finalités explicites et déterminées, et uniquement pour des finalités ultérieures compatibles avec la finalité initiale (Convention 108+, article 5.4.*c*). Le traitement ultérieur des données ne peut donc pas être effectué d'une manière inattendue, inappropriée ou répréhensible pour la personne concernée.

Pour évaluer si le traitement ultérieur doit être considéré comme compatible, le responsable du traitement devrait tenir compte, entre autres, de la nature des données à caractère personnel, des conséquences du traitement ultérieur envisagé pour les personnes concernées, du contexte dans lequel les données à caractère personnel ont été recueillies, en particulier concernant les attentes raisonnables des personnes concernées fondées sur la relation avec le responsable du traitement quant à leur utilisation ultérieure, et/ou l'existence de garanties appropriées dans les opérations de traitement ultérieures initiales et prévues[13].

Si la finalité du traitement ultérieur est incompatible avec la finalité initiale, le responsable du traitement est tenu d'informer les personnes concernées afin soit d'obtenir leur consentement, si les conditions d'un consentement valable sont remplies en ce qui concerne la finalité supplémentaire, soit de disposer d'une autre base juridique pour le traitement ultérieur.

13. Rapport explicatif de la Convention 108+, par. 49.

Dans le contexte de la LBC/FT[14]

Les données à caractère personnel sur le client, ou les données transactionnelles qui peuvent être collectées par les entités assujetties à des fins de vigilance à l'égard de la clientèle, peuvent – dans certaines conditions prévues par la loi – être partagées avec d'autres entités obligées appartenant au même groupe, afin de remplir des finalités compatibles supplémentaires (par exemple informer une entité assujettie appartenant au même groupe au sujet d'un client commun qui peut avoir fait l'objet d'une déclaration à la CRF). Par exemple dans les relations de correspondance bancaire, la banque correspondante peut avoir besoin d'exiger des informations supplémentaires concernant un client de la banque répondante, qui auraient été recueillies par cette banque auprès de son client dans un contexte différent. Il peut parfois être nécessaire de partager des données même avec des tiers[15], lorsque cela est strictement nécessaire pour remplir les obligations de vigilance à l'égard de la clientèle. Ces opérations doivent être effectuées dans le respect des obligations de secret et des règles applicables en matière de protection des données à caractère personnel.

En tant qu'élément de contexte, il est important de faire la distinction entre le partage de données par les CRF avec d'autres organismes répressifs nationaux et avec des CRF étrangères aux fins de la coopération internationale, car des règles différentes peuvent s'appliquer et le principe de limitation de la finalité doit être suivi de près.

Parfois, des données collectées et traitées dans un but précis (par exemple des informations sur la vigilance à l'égard de la clientèle ou des informations sur des transactions suspectes) doivent être partagées avec des tiers. Par exemple une CRF qui analyse une déclaration d'opération suspecte (DOS) peut trouver des liens internationaux nécessitant un partage d'informations pertinentes figurant dans la DOS (y compris des données à caractère personnel) auprès d'une autre autorité compétente ou d'une CRF étrangère dans le cadre d'une demande d'information complémentaire.

À l'occasion, l'entité assujettie peut avoir besoin de déposer une déclaration d'opération suspecte auprès de la CRF. Le traitement des données à caractère personnel par la CRF constitue dans ce cas une finalité supplémentaire qui est considérée comme compatible avec la finalité initiale du traitement. La CRF peut en outre être amenée à signaler une suspicion d'activité criminelle à une

14. Recommandations pertinentes du GAFI : 10-12, 13, 15-18, 20, 22-25, 27, 29, 31, 40.
15. Dans ce contexte, le terme « tiers » devrait être interprété comme toute personne physique ou morale qui est extérieure à l'entité assujettie ou à son établissement financier et qui n'en fait pas partie.

autorité compétente. Le traitement des dossiers par les autorités compétentes en matière d'enquête et de poursuites est généralement régi par d'autres lois.

Les données à caractère personnel doivent être utilisées aux seules fins pour lesquelles elles ont été fournies et ne peuvent être transférées à d'autres autorités des pays destinataires des données, sauf si les exigences énoncées dans la Convention 108+ sont respectées.

Recommandations

Le principe de limitation de la finalité doit être respecté, tant lorsque le traitement des données est effectué pour plusieurs finalités différentes que lorsqu'il est effectué pour une finalité compatible. La notion d'utilisation compatible ne doit pas nuire à la transparence, à la sécurité juridique, à la prédictibilité et à la loyauté du traitement des données[16].

Les entités assujetties appartenant à un groupe doivent disposer de politiques et de procédures claires, fondées sur la loi, pour définir quel type de données à caractère personnel (client, bénéficiaire effectif, transactionnel, compte, DOS) elles peuvent échanger entre elles[17], sur quelle base juridique et dans quel but. Cela pourrait être fait conformément à l'article 14 de la Convention 108+, y compris les garanties standards approuvées telles que des règles d'entreprise contraignantes, ou des clauses ad hoc venant d'instruments légalement contraignants en vigueur.

Les CRF, pour le traitement de données à caractère personnel dans les DOS, devraient disposer de règles et de procédures claires, fondées sur la loi, qui devraient également prescrire les finalités pour lesquelles les données à caractère personnel relatives aux DOS peuvent être partagées avec d'autres autorités compétentes[18].

Lorsque des données à caractère personnel sont traitées dans le cadre d'un scénario de dépendance[19] à l'égard de tiers[20], les deux parties devraient avoir mis en place des règles et des procédures claires qui régissent non seulement la fourniture d'informations à des fins de vigilance à l'égard de la

16. Rapport explicatif de la Convention 108+, par. 49.
17. GAFI, recommandation 18 ; Convention108+ : articles 5.1, 14.2 et 3 ; par. 40, 42, 109-111 du rapport explicatif.
18. GAFI, recommandation 29 ; Convention108+ article 10 ; par. 85 du rapport explicatif.
19. Dans ce contexte, le terme « tiers » désigne les institutions financières ou les EPNFD qui sont supervisées ou surveillées et qui satisfont aux exigences de la recommandation n°17 du GAFI.
20. Dans ce contexte, le terme « tiers » désigne les institutions financières ou les EPNFD qui sont supervisées ou surveillées et qui satisfont aux exigences de la recommandation n°17 du GAFI.

clientèle, mais aussi des garanties adéquates pour la protection des données à caractère personnel traitées à des fins particulières.

En ce qui concerne les relations de correspondance bancaire et les autres relations similaires[21], il faudra prévoir des dispositions claires et détaillées, fondées sur la loi, entre le correspondant et la banque répondante pour réglementer le partage par la banque répondante des données à caractère personnel concernant ses clients, ses bénéficiaires effectifs et ses opérations. Des dispositions devraient également détailler le type de données que la banque répondante devra fournir à la demande de la banque correspondante. Il peut en aller de même pour des relations similaires pertinentes en dehors du secteur bancaire (par exemple entreprises d'investissement, établissements de paiement). Des orientations à cet égard devraient être fournies par les autorités chargées de la protection des données.

Il convient aussi de mettre en œuvre, conformément à l'article 5.4.*c* de la Convention 108+, le principe de limitation de la finalité également dans le contexte du partage/transfert de données par les CRF avec d'autres destinataires y compris des services répressifs nationaux[22], mais aussi avec les CRF étrangères[23] . Dans ce cas, des procédures pour la mise en œuvre des normes internationales devraient être élaborées pour garantir que les données soient partagées pour une finalité spécifique et limitée, et documentées au cours du transfert, et qu'une protection essentielle équivalente soit assurée pendant le transfert ainsi que par les autorités destinataires.

3.2. La licéité du traitement – Base juridique

Principe général

Conformément aux obligations de l'article 5, alinéas 2 et 3, de la Convention 108+, le traitement des données à caractère personnel doit être licite, c'est-à-dire reposer soit sur le consentement de la personne concernée, soit sur un fondement légitime prévu par la loi.

Pour être valable, le consentement doit être : (i) libre, (ii) spécifique, (iii) éclairé et (iv) non équivoque et révocable à tout moment – éléments explicités dans le rapport explicatif[24].

21. GAFI, recommandation 13 ; et Convention108+, articles 14.2 et 14.3 ; par.109 à 111 du rapport explicatif.
22. GAFI, recommandations 29 et 31.
23. GAFI, recommandation 40 ; et Convention108+, articles 14.2 et 14.3 ; par.109 à 111 du rapport explicatif.
24. Convention 108+, article 5.2 ; rapport explicatif de la Convention 108+, par. 42 à 45.

La notion de « fondement légitime prévu par la loi », au paragraphe 2, englobe notamment les traitements de données nécessaires : (i) à l'exécution d'un contrat auquel la personne concernée est partie ; (ii) à la protection d'intérêts vitaux de la personne concernée ou d'une autre personne ; (iii) à la mise en conformité avec une obligation légale incombant au responsable du traitement ; (iv) pour des motifs d'intérêt public ou (v) pour des intérêts légitimes prédominants du responsable du traitement ou d'un tiers.

Quelle que soit la base juridique invoquée par le responsable du traitement, les catégories particulières de données, notamment, doivent faire l'objet de garanties supplémentaires telles que prévues à l'article 6 de la Convention 108+, notamment sur le consentement explicite.

Dans le contexte de la LBC/FT[25]

Le traitement des données dans le cadre de la LBC/FT doit reposer sur une base juridique claire et détaillée, et être nécessaire et proportionné au but légitime poursuivi.

Comme déjà expliqué, pour constituer une base juridique au traitement de données à caractère personnel, le consentement doit être libre, éclairé, spécifique et non équivoque ; le consentement au traitement doit être clairement affirmé. Dans le contexte de la LBC/FT, la question d'un consentement « librement » donné devrait être examinée attentivement et il convient de veiller à ce que la personne concernée ait le choix. Si tel n'est pas le cas, le traitement des données doit être fondé sur une base juridique différente et valable. Le cadre LBC/FT suppose souvent des investigations spécifiques sur les activités de BC/FT établies ou soupçonnées, prévoit des situations où le client n'est pas ou pas seulement partiellement informé du traitement des données, en particulier en ce qui concerne les obligations de déclaration des transactions suspectes par l'entité assujettie, la fourniture de données à caractère personnel en réponse aux demandes d'informations des CRF et des services répressifs et de supervision, et l'application des ordonnances de contrôle. Dans ces cas, l'information préalable du client contredirait les interdictions associées à la LBC/FT, en particulier l'interdiction de divulgation[26].

Le motif licite autorisant les pouvoirs publics à traiter des données à caractère personnel peut être celui de l'intérêt public, dans la mesure où ils sont investis du pouvoir de lutter contre le BC/FT et de fonctions spécifiques dans ce domaine. Des mécanismes régulateurs ainsi qu'un contrôle sont également mis en œuvre. Il n'en va cependant pas de même pour les institutions du secteur privé, qui sont des entités obligées et ne bénéficient ni du même statut juridique, ni du même mandat.

25. Recommandations pertinentes du GAFI : 24, 25.
26. Recommandation du GAFI 21.

Le traitement de données à caractère personnel par des entités assujetties dans le cadre de la LBC/FT devrait reposer sur une base juridique claire et détaillée qui énonce les principes de nécessité et de proportionnalité auxquels sont soumis les responsables du traitement[27]. Une entité assujettie qui ne respecterait pas ces obligations s'expose à des mesures de la part des autorités chargées de la protection des données, notamment des sanctions administratives ou pénales. La non-fourniture par le client des données demandées peut avoir deux conséquences : l'interruption de la transaction ou de la relation client, ou la restriction des prestations fournies.

Par exemple le traitement des données est nécessaire pour éviter l'utilisation de personnes morales et de constructions juridiques à des fins de BC ou de FT, en assurant des informations satisfaisantes, exactes et à jour sur les bénéficiaires effectifs et sur le contrôle des personnes morales et constructions juridiques[28]. Les informations sur les bénéficiaires effectifs d'une société devraient être accessibles en temps opportun par une autorité compétente, soit par un registre de propriété effective ou un mécanisme alternatif. Dans le même temps, lorsqu'elles donnent accès aux informations de bénéficiaires effectifs, les autorités compétentes devraient dûment tenir compte du droit au respect de la vie privée des personnes concernées, en tenant compte de leurs droits et libertés et en ayant une incidence sur ces droits.

L'existence d'initiatives de partage de l'information par le biais de partenariats public-privé (PPP) a été notée dans plusieurs administrations. Si les possibilités que ces partenariats offrent dans la lutte contre la criminalité financière sont importantes, il reste des défis qui sont également de nature législative et de conformité (par exemple des modifications législatives peuvent être nécessaires pour garantir une base juridique appropriée et permettre aux partenaires d'atteindre leurs objectifs).

Recommandations

Le traitement des données dans le contexte LBC/FT devrait être effectué sur la base d'un fondement légal clair et détaillé respectant les principes de nécessité et de proportionnalité, et avec des garanties appropriées.

Il convient de tenir dûment compte du mandat confié aux autorités publiques et de leur obligation de répondre du non-respect de leurs obligations légales. La question de l'intérêt public comme base juridique d'initiatives émergentes de traitement des données par des entités du secteur privé soumises à des obligations de LBC/FT devrait être dûment motivée et soigneusement examinée.

27. Rapport explicatif de la Convention 108+, par. 46.
28. GAFI, recommandation 24.

Des dispositions claires et détaillées qui tiennent compte de tous les droits et intérêts concernés sont établies en ce qui concerne les PPP créés pour le partage d'informations opérationnelles sur les renseignements concernant les suspects, y compris en ce qui concerne les données à caractère personnel partagées par les autorités répressives et la base juridique claire pour le traitement ultérieur. Ces règles devraient spécifier les conditions du traitement, y compris : les finalités spécifiques pour lesquelles le partage de données et d'autres traitements sont autorisés ; l'ensemble de données nécessaire à soumettre par l'entité assujettie en veillant à ce que seules les données à caractère personnel strictement nécessaires à l'analyse opérationnelle ou à l'enquête en cours soient divulguées et partagées; les garanties appropriées pour garantir les droits des personnes concernées; les garanties appropriées, complétant celles de la convention pour des catégories spéciales de données.

En ce qui concerne les registres centraux des bénéficiaires effectifs, les données à caractère personnel ne devraient être disponibles que dans les situations ou dans la mesure prévue par la loi, et conformément aux normes et réglementations internationales en matière de protection des données.

3.3. La loyauté et la transparence des principes de traitement

Principe général

Les données à caractère personnel sont traitées de manière non seulement licite, mais aussi loyale, tant par le responsable du traitement que par le sous-traitant (article 5.4 de la Convention 108+). Ce principe requiert la communication à la personne concernée d'informations sur le traitement de ses données, y compris sur les risques éventuellement identifiés par le responsable ou le sous-traitant, pour lui permettre de prendre une décision éclairée et d'exercer ses droits en matière de protection des données, sauf si une exception s'applique conformément à la convention. En outre, l'équité exige également d'évaluer les conséquences que le traitement des données aura sur la personne concernée. Les opérations de traitement ne sauraient être réalisées en secret.

Le principe de transparence est intimement lié au principe de loyauté. Le traitement des données est effectué de manière transparente à l'égard de la personne concernée (articles 5.4.*a* et 8 de la Convention 108+). De ce fait, les personnes concernées doivent être informées avant le traitement de leurs données, notamment, des catégories de données à caractère personnel traitées, de la finalité du traitement et de l'identité et de l'adresse du

responsable du traitement. En cas de responsabilité conjointe, les responsables du traitement doivent clarifier toutes les finalités du traitement conjoint et les moyens, procédures et modalités d'exercer les droits énoncés à l'article 9, pour assurer la transparence[29]. Ce faisant, il faut tenir compte du fait que les pouvoirs publics et les entités du secteur privé n'ont pas les mêmes statuts et obligations juridiques, et qu'ils peuvent donc relever de différents régimes de protection des données.

Les informations sur le traitement des données doivent être fournies dans un langage clair et simple, permettant aux personnes concernées de comprendre facilement les risques, les garanties et les droits en jeu (sauf si une exception prévue à l'article 11 s'applique). En outre, la personne concernée doit être informée de ses droits, dont celui de demander au responsable si des données la concernant sont traitées et, dans l'affirmative, quelle est la nature des données qui font l'objet de ce traitement (article 9.1.*b* de la Convention 108+).

Dans le contexte de la LBC/FT[30]

Le traitement de données à des fins d'intérêt public ne devrait pas être par définition considéré comme loyal : les responsables du traitement relevant du secteur public doivent observer ces principes, sauf si une exception s'applique conformément à l'article 11 de la Convention 108+.

Les entités assujetties sont obligées[31] de prendre des mesures de vigilance à l'égard de leur clientèle dans les cas suivants : (i) par exemple lorsqu'elles établissent des relations d'affaires ; (ii) elles effectuent des opérations occasionnelles supérieures au seuil désigné applicable ; (iii) elles effectuent des opérations occasionnelles sous forme de virements électroniques[32] ; (iv) il existe un soupçon de BC/FT ; ou (v) elles doutent de la véracité ou de la pertinence des données d'identification personnelle. Il appartient aux entités assujetties d'identifier le client (personne physique ou morale, ou structure permanente ou occasionnelle) et de vérifier son identité au moyen de sources fiables et indépendantes[33]. Elles doivent aussi vérifier que toute personne prétendant agir pour le compte du client ou du bénéficiaire effectif est autorisée à le faire, et identifier et vérifier l'identité de cette personne. Les entités assujetties, en particulier les banques, informent généralement leur clientèle des finalités pour lesquelles ses données seront traitées et, le cas échéant, partagées avec

29. Comité européen de la protection des données, « Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD », version 2.0, 7 juillet 2021.
30. Recommandations pertinentes du GAFI : 10, 22 et 23.
31. La recommandation 10 du GAFI fait de ces mesures la norme minimale que les pays devraient mettre en place.
32. Dans ces circonstances, voir la recommandation 16 du GAFI sur les virements électroniques.
33. GAFI, recommandation 10.

des tiers, et requièrent son consentement, bien que cela ne fasse pas partie des exigences du GAFI et que les pratiques varient d'un pays à l'autre, en fonction de la législation locale sur la protection des données. Dans certaines circonstances spécifiques, les entités assujetties peuvent aussi requérir le consentement d'un client, en particulier pour la prestation de certains services ou à l'occasion de la divulgation à des tiers de données relatives à la clientèle.

Dans certains cas, outre la réglementation sur la protection des données, il existe des obligations de secret bancaire[34] ou d'autres obligations de secret professionnel qui s'appliquent à des professionnels du droit tels que les avocats, les notaires, les autres professionnels juridiques indépendants et les comptables agissant à titre de professionnels juridiques indépendants. Ils ne sont pas tenus de signaler les transactions suspectes ou de fournir des informations sur les clients aux forces de l'ordre ou aux CRF lorsque ces informations seraient obtenues: a) dans le cadre de l'évaluation de la situation juridique de leur client, ou b) dans l'exercice de leur mission de défense ou de représentation de leur client ou concernant des procédures judiciaires, administratives, arbitrales ou de médiation[35].

Afin de faciliter l'accès à des informations précises et actualisées sur la propriété effective, certains États ont créé des registres centraux comprenant des informations fournies par des personnes morales et des constructions juridiques. L'accès à ces informations est généralement donné aux entités assujetties aux fins de diligence raisonnable ainsi qu'aux autorités compétentes, en particulier la CRF. L'accès à ces informations est important, notamment pour les autorités chargées des enquêtes et des poursuites, afin de retracer les activités criminelles.

Recommandations

Lorsqu'elles établissent des relations commerciales avec des clients ou effectuent des transactions pour des clients occasionnels, les entités assujetties, dans leur rôle de responsables du traitement, devraient communiquer à la personne concernée, entre autres, des informations concernant la base juridique et les finalités du traitement envisagé, les catégories de données que l'IF et l'EPNFD (ou d'autres tiers) traiteront, les destinataires ou les catégories de destinataires des données à caractère personnel, le cas échéant ; les moyens d'exercer les droits énoncés à l'article 9 de la Convention 108+ et les restrictions éventuelles, en cas de besoin, ainsi que toute information supplé-

34. La recommandation 9 du GAFI stipule que les lois sur le secret des institutions financières ne doivent pas entraver la mise en œuvre des recommandations du GAFI.
35. GAFI, recommandation 23.

mentaire nécessaire pour assurer un traitement équitable et transparent des données à caractère personnel et l'utilisation qui en est faite, d'une manière compréhensible et conviviale.

- La loi doit instaurer une obligation légale claire prévoyant, le cas échéant, que les données des clients peuvent être divulguées à des tiers en dépit des règles de confidentialité.

- L'accès public par défaut aux données à caractère personnel des registres centraux des bénéficiaires effectifs constitue une ingérence grave dans les droits de l'homme, y compris le droit à la vie privée et à la protection des données à caractère personnel, et ne devrait être autorisé que dans les situations ou dans la mesure prévues par la loi, et dans le respect des réglementations en matière de protection des données, notamment pour ce qui est des principes de nécessité, de proportionnalité et de limitation. L'accès aux données non accessibles au public est géré avec soin en tenant compte de la législation nationale, des droits et des intérêts concernés.

3.4. Le principe de la minimisation des données

Principe général

- Le traitement des données doit être limité à ce qui est nécessaire pour atteindre une finalité légitime et prédéterminée (article 5.4.*c*). Un responsable du traitement des données devrait limiter strictement la collecte des données aux informations directement pertinentes au regard de la finalité spécifique poursuivie par le traitement, y compris concernant la collecte et le traitement de données par un ou de multiples sous-traitants.

- Pour appliquer ce principe, le responsable doit vérifier la nécessité du traitement des données et sa proportionnalité à la finalité spécifique, ainsi que l'existence d'autres moyens moins intrusifs. S'agissant de la nécessité, par exemple, les responsables déterminent si l'objectif pourrait être atteint en traitant des données anonymes. S'agissant de la proportionnalité, le volume de données à collecter est soigneusement étudié à l'aune de la finalité du traitement, en tenant dûment compte du principe de la minimisation des données.

Dans le contexte de la LBC/FT

- Les lois sur la LBC/FT peuvent prévoir différents niveaux de traitement des données à caractère personnel (données de vigilance à l'égard de la clientèle) par les entités assujetties, notamment une diligence raisonnable simplifiée, normale et renforcée à l'égard des clients. En principe, le renforcement de la diligence raisonnable exige le traitement d'une plus grande quantité de données à caractère personnel, y compris la vérification de ces données à partir de diverses sources accessibles à l'entité assujettie. Une diligence renforcée peut

être exigée en fonction des risques que posent certains types de clients (par exemple les personnes politiquement exposées (PPE[36]) ou lorsque les risques liés au BC/FT sont plus grands) ou certains types de services ou de transferts (par exemple les transferts de capitaux vers des pays à haut risque), voire des clients particuliers dans des situations où des risques ou des transactions suspectes ont été détectés. Les lois sur la LBC/FT peuvent prévoir différentes périodes de conservation des données pour différents types de données à caractère personnel.

En pratique, il s'avère que, dans de nombreux cas, les entités du secteur privé manquent d'orientations claires et spécifiques nécessaires à la collecte des données à caractère personnel de leurs clients dans le cadre de leurs obligations de LBC/FT. Lorsqu'elles collectent, par exemple, des jeux de données spécifiques dans le cadre des obligations de vigilance à l'égard de la clientèle, les entités assujetties doivent observer des obligations juridiques de protection des données et des obligations LBC/FT, et peuvent rencontrer des difficultés à comprendre comment atteindre ces deux buts de manière cohérente et compatible, en particulier eu égard au principe de minimisation des données. Par conséquent, par crainte de s'exposer à des risques de réputation et autres causés par (i) le traitement involontaire de produits du crime, ou (ii) la possibilité de faire l'objet d'amendes administratives ou de mesures de la part des institutions de contrôle compétentes tant des IF que des EPNFD, les entités du secteur privé peuvent finir par partager « au cas où » un plus grand volume de données. En ce sens, la mise en œuvre correcte d'une approche fondée sur les risques du point de vue de la LBC/FT permettrait également de s'aligner sur l'exigence de proportionnalité envisagée dans les exigences en matière de protection des données. L'application efficace d'une approche fondée sur les risques nécessite des orientations et une formation claires et pratiques de la part des autorités de contrôle, des investissements dans les ressources et l'expertise par les entités assujetties, ainsi qu'une application et une mise en œuvre proportionnées des lois nationales en matière de LBC/FT.

Recommandations

Le traitement des données par les entités assujetties doit être limité à ce qui est directement pertinent pour la finalité spécifique poursuivie compte tenu des risques inhérents à la relation client.

36. Selon les normes du GAFI, les personnes politiquement exposées (PPE) sont classées comme suit : (i) PPE étrangères, (ii) PPE nationales, et (iii) personnes qui sont ou ont été chargées d'une fonction importante par une organisation internationale. Elles désignent les membres de la haute direction, c'est-à-dire les administrateurs, les directeurs adjoints et les membres du conseil d'administration ou des fonctions équivalentes. La définition des PPE ne vise pas les personnes de rang intermédiaire ou plus subalterne dans les catégories susmentionnées. Voir annexe pour plus de détails.

- En ce qui concerne le traitement des données par le secteur privé, les ensembles de données spécifiques à collecter dans le cadre des obligations en matière de LBC/FT ne sont pas toujours précisés par le droit interne, notamment en ce qui concerne l'approche fondée sur les risques, qui nécessite une certaine flexibilité, alors que le principe de minimisation des données est clairement prévu par le droit interne sur la protection des données. Il est donc recommandé de faciliter la collaboration entre les autorités nationales, régionales et internationales de protection des données, les autres autorités chargées de la protection des données, financières ou non (EPNFD) et les forums internationaux de LBC/FT, afin que des orientations spécifiques puissent être élaborées pour assurer une cohérence entre les obligations légales applicables.

- Dans le cadre du traitement automatisé des données (au niveau de la collecte mais aussi des transferts de données), une approche de protection de la vie privée dès la conception devrait être mise en œuvre (tant par le secteur privé que par les autorités répressives, y compris les CRF) et intégrer la minimisation des données dans l'architecture du système utilisé (par exemple champs de données obligatoires limités, zones de texte libre limitées, etc.) conformément à l'article 10 de la Convention 108+. À cet égard, les responsables du traitement et, le cas échéant, les sous-traitants devraient veiller à ce que les exigences en matière de protection des données soient intégrées idéalement au stade de l'architecture et de la conception du système, dans les opérations de traitement des données, au moyen de mesures techniques et organisationnelles.

- Dans le cadre du PPP, le partage de données de transaction impliquant le traitement d'une grande quantité de données, le traitement devrait être effectué, le cas échéant, avec des données anonymisées ou pseudonymisées. L'identification d'une personne relativement à une transaction ne devrait être limitée que lorsque le résultat du traitement fondé sur des conditions liées à un soupçon raisonnable/une cause probable révèle des schémas, *modus operandi* ou des activités concrètes qui pourraient nécessiter la déclaration de l'opération à la CRF comme étant suspecte, ou lorsqu'il est nécessaire d'identifier des liens avec un terroriste identifié. Par exemple lorsque le traitement des données est effectué pour identifier des tendances, des modèles et des typologies, il n'est pas nécessaire d'utiliser des données à caractère personnel.

- Le principe de minimisation des données devrait également être appliqué dans le contexte du traitement automatisé des données lors de la collecte des données, mais aussi au niveau des transferts de données.

3.5. Le principe de l'exactitude des données

Principe général

Le principe d'exactitude des données est mis en œuvre par le responsable du traitement dans toutes les opérations de traitement (article 5.4.*d*). On attend des responsables qu'ils prennent des mesures raisonnables pour veiller à ce que les données collectées soient exactes et, si nécessaire, vérifier régulièrement qu'elles sont à jour, en fonction de la finalité spécifique. Les données inexactes doivent être effacées ou rectifiées. Il appartient donc aux responsables de réagir lorsque des personnes concernées demandent la correction des fichiers inexacts ou incomplets.

Lorsqu'il a été nécessaire de corriger des données inexactes, il pourrait être acceptable que les responsables du traitement conservent une trace des événements qui se sont produits par erreur, à condition que ces notes ne prêtent pas à confusion quant aux faits et qu'elles se limitent à décrire l'événement, la date et la cause de la correction.

À la phase de collecte des données, les responsables évaluent la fiabilité de la source d'information. Lors du traitement ultérieur, et en fonction de la finalité spécifique, l'exactitude des données à caractère personnel doit être régulièrement vérifiée, afin de prévenir toute conséquence préjudiciable à la personne concernée.

Dans le contexte de la LBC/FT[37]

Les entités assujetties doivent s'assurer que les documents, données et informations obtenues dans l'exercice du devoir de vigilance restent à jour et pertinents. Cela implique d'examiner les éléments existants et d'effectuer des opérations de suivi récurrentes, sur une base régulière, pour les catégories de clients présentant des risques plus élevés[38].

Les entités assujetties peuvent faire appel à des prestataires externes à diverses fins d'informations (par exemple vérification des sanctions, identification des PPE, des membres de la famille et des proches) qui, si elles sont fournies avec des données à caractère personnel inexactes ou obsolètes, peuvent donner des résultats inexacts en termes de vigilance à l'égard de la clientèle ou d'autres fins de LBC/FT (par exemple le suivi). Elles peuvent recourir à des systèmes fondés sur l'intelligence artificielle (IA) pour surveiller les transactions afin d'identifier des modèles et des tendances suspects, et

37. Recommandations pertinentes du GAFI : 6, 7, 10, 17, 24, 37, 40.
38. GAFI, recommandation 10.

générer des alertes qui, si elles n'utilisent pas des données précises et ne sont pas correctement calibrées, risquent de devenir des données faussement positives, des cas non détectés et/ou trop nombreux, et ne peuvent pas être traitées de manière légale. Bien que les recommandations du GAFI fassent référence à l'exigence de garantir l'exactitude des informations, les implications concrètes de la vérification de l'exactitude de toutes les données à caractère personnel restent à déterminer, l'obligation susmentionnée de tenir à jour des données et informations de vigilance à l'égard de la clientèle s'applique même aux données collectées auprès de fournisseurs externes.

Les entités assujetties sont autorisées à s'appuyer sur des tiers pour l'exécution de certains éléments du processus de vigilance à l'égard de la clientèle[39]. Le fait que les informations de vigilance à l'égard de la clientèle aient été collectées et traitées par une tierce partie sur laquelle l'entité assujettie n'a pas de contrôle peut entraîner des inexactitudes dans les informations collectées pour le processus de vigilance. Cependant, les normes du GAFI indiquent clairement que la responsabilité de l'accomplissement de l'obligation de vigilance à l'égard de la clientèle incombe à l'entité assujettie qui se fie à la tierce partie. Cela est cohérent avec le rôle du responsable du traitement des entités assujetties, tel que défini dans la Convention 108+. Par conséquent et sur la base des recommandations du GAFI impliquant de vérifier toutes les données à caractère personnel, l'obligation susmentionnée de maintenir à jour les données et informations de vigilance s'applique même aux situations où l'on se fie à des tiers.

Les pays sont tenus de mettre en place des mécanismes pour s'assurer que les informations sur les bénéficiaires effectifs sont obtenues par l'entreprise ou autrement disponibles en temps opportun[40]. Dans la pratique, les lois sur la LBC/FT exigent généralement la même chose pour les autres entités juridiques inscrites dans les registres des bénéficiaires effectifs. En outre, les données de base (c'est-à-dire le nom de la société, la preuve de sa constitution, sa forme et son statut juridique, l'adresse du siège social, les pouvoirs réglementaires de base et la liste des administrateurs) doivent être accessibles au public dans un registre de société, et prévoient également la possibilité d'exiger des sociétés ou des registres de sociétés qu'ils obtiennent et détiennent des informations sur les bénéficiaires effectifs[41].

Les pays sont tenus d'accorder de manière rapide, constructive et efficace la coopération internationale la plus large possible sur les informations de base et celles relatives aux bénéficiaires effectifs, notamment en échangeant des informations sur les actionnaires et sur les bénéficiaires effectifs[42].

39. GAFI, recommandation 17.
40. GAFI, recommandation 24.
41. *Ibid.*
42. GAFI, recommandations 37 et 40.

Recommandations

Les entités assujetties devraient mettre en œuvre des procédures pour s'assurer qu'elles respectent l'exigence d'exactitude énoncée à l'article 5, paragraphe 4.*d*, dans toute opération de traitement de données de vigilance à l'égard de la clientèle, afin d'éviter les risques et les effets préjudiciables sur les droits du client en tant que personne concernée, qui peuvent résulter du traitement de données qui ne sont pas à jour.

Lorsque l'IA est utilisée (par exemple pour le suivi des transactions dans le but de détecter une activité suspecte), il est important que cela soit réalisé dans le strict respect des règles relatives à la protection des données, notamment concernant les obligations énoncées à l'article 10.3, pour que les responsables du traitement et, le cas échéant, les sous-traitants mettent en œuvre des mesures techniques et organisationnelles en tenant compte des implications du droit à la protection des données à caractère personnel à toutes les étapes du traitement. Par ailleurs, la personne concernée ne doit pas être soumise à une décision l'affectant de manière significative, qui serait uniquement fondée sur un traitement automatisé de données, sans que son point de vue soit pris en compte, sauf si le traitement des données est autorisé par la loi à laquelle le responsable du traitement est soumis et qui prévoit des mesures appropriées pour sauvegarder les droits, libertés et intérêts légitimes de la personne concernée. Cela implique que, sur la base d'une demande de la personne concernée, une intervention humaine est nécessaire de la part d'un membre du personnel collectant l'information pour vérifier l'exactitude des résultats (par exemple pour éviter tout impact négatif sur les personnes concernées en cas de décision fondée sur un faux positif obtenu uniquement par des moyens automatisés). Les garanties pourraient inclure l'obligation : a) de fournir les informations supplémentaires nécessaires aux personnes concernées ; b) d'assurer un traitement équitable et transparent ; c) de mettre en évidence l'utilisation d'un traitement uniquement automatisé ainsi que son objectif et son impact potentiel sur la personne concernée conformément à l'article 8.1 et à l'article 9.1.*b*. En outre, les critères de traitement doivent être calibrés de manière à ne pas générer un nombre excessif d'alertes, en particulier de faux positifs, y compris dans le cas de la recherche du nom du client/du bénéficiaire effectif/du destinataire de la transaction, et de leur correspondance avec les listes de sanctions[43].

43. GAFI, recommandations 6 et 7 ; Convention108+, articles 9.*a* et 10.1 ; par. 71-73, 75 et 85 du rapport explicatif.

- Si les entités assujetties utilisent des systèmes automatisés, y compris gérés par un traitement algorithmique ou l'intelligence artificielle pour le profilage du risque des clients ou des bénéficiaires effectifs, des mesures appropriées doivent être prises pour corriger les facteurs d'inexactitude des données et limiter les risques d'erreurs inhérents au profilage. La réévaluation périodique (ou fondée sur un élément déclencheur) doit également inclure une réévaluation des données et des déductions statistiques, y compris pour l'élimination des biais potentiels utilisés pour le profilage du risque, afin de déterminer si elles sont toujours exactes et pertinentes. En ce qui concerne le traitement des données à caractère personnel par les nouvelles techniques et technologies de traitement, les entités assujetties sont invitées à suivre la Recommandation CM/Rec(2021)8 du Comité des Ministres aux États membres sur la protection des personnes physiques à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage[44] et les Lignes directrices sur l'intelligence artificielle et la protection des données[45].

- Si les entités assujetties font appel à des fournisseurs de bases de données externes pour mettre en œuvre des mesures à l'égard des bénéficiaires effectifs de leurs clients (par exemple la vérification de l'identité du client et du bénéficiaire effectif, l'identification des relations potentielles avec les PPE, ainsi que des membres de la famille et des proches de la PPE), elles devraient vérifier que les données à caractère personnel utilisées sont exactes et à jour, et procéder à une évaluation périodique de l'exactitude des données mises à disposition par le fournisseur.

- Les pays devraient veiller à l'existence de politiques obligeant les responsables des registres des sociétés à vérifier la qualité des données à caractère personnel inscrites sur ces registres ou à employer d'autres moyens appropriés pour s'assurer que les données sont exactes et à jour.

- L'entité assujettie qui reçoit des données spécifiques sur les clients, les bénéficiaires effectifs et les transactions dans des buts spécifiques est considérée comme le responsable du traitement et doit être tenue responsable de leur traitement comme de leur exactitude, même lorsqu'elle fait appel à des tiers pour la collecte et le traitement. Ces tiers peuvent être considérés comme des responsables du traitement au sens de la Convention 108+.

- Conformément à l'article 10 de la Convention 108+, les entités assujetties doivent mettent en œuvre des mesures visant à prévenir ou minimiser le risque d'ingérence dans les droits et libertés fondamentales des clients.

44. Recommandation CM/Rec (2021)8.
45. https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b8

Les entités assujetties sont invitées à adopter une approche de confidentialité dès la conception pour le traitement des données à caractère personnel y compris durant la phase d'intégration et d'automatisation de la mise à jour.

Sans préjudice des normes en matière de protection et de sécurité des données, afin de faciliter une coopération internationale rapide, constructive et effective, les données conservées ou obtenues aux fins d'identification des bénéficiaires effectifs devraient être facilement accessibles.

3.6. Le principe de la limitation de la conservation

Principe général

L'article 5.4.*e* de la Convention 108+ exige que les données à caractère personnel soient effacées ou rendues anonymes dès qu'elles ne sont plus nécessaires pour les finalités pour lesquelles elles ont été collectées. Il existe toutefois des exceptions à ce principe à condition (i) qu'elles soient prévues par la loi ; (ii) qu'elles respectent l'essence des droits et libertés fondamentaux ; et (iii) qu'elles soient nécessaires et proportionnées à la poursuite d'un nombre limité d'objectifs légitimes (article 11). Il s'agit, entre autres, de la préservation de la sécurité nationale, des enquêtes sur les infractions pénales et leur poursuite, de la protection de la personne concernée et de la protection des droits et des libertés fondamentales d'autrui.

Dans le contexte de la LBC/FT[46]

Des exigences claires sont définies en matière de durée de conservation des informations relatives à la vigilance à l'égard de la clientèle, des dossiers de comptes, de la correspondance commerciale et des résultats de toute analyse entreprise (actuellement requis pour au moins cinq ans après la fin de la relation d'affaires ou après la transaction occasionnelle) et des dossiers sur les transactions internes ou internationales (au moins cinq ans après la fin de la transaction)[47].

Le traitement des données est nécessaire pour éviter l'utilisation de personnes morales et de constructions juridiques à des fins de BC ou de FT, en assurant des informations satisfaisantes, exactes et à jour sur les bénéficiaires effectifs et sur le contrôle des personnes morales et des constructions juridiques[48]. En cas de cessation d'existence (dissolution ou autre) d'une société, toutes les parties prenantes et la société elle-même (ou ses dirigeants,

46. Recommandations pertinentes du GAFI : 2, 11, 24, 25, 29, 40.
47. GAFI, recommandation 11.
48. GAFI, recommandations 24 et 25.

liquidateurs ou autres personnes impliquées dans sa dissolution) sont tenues de conserver les informations et pièces mentionnées pendant au moins cinq ans après la date à laquelle la société est dissoute ou cesse d'exister, ou pendant au moins cinq ans après la date à laquelle la société cesse d'être cliente de l'intermédiaire professionnel ou de l'institution financière.

Lorsque la législation impose une période de conservation spécifique, les responsables doivent adopter les mesures nécessaires pour garantir une protection adéquate des données.

Recommandations

Conformément à l'article 5.4.*e* de la Convention 108+, les données à caractère personnel ne doivent être conservées, en principe, que pour la durée minimale nécessaire, et être supprimées ou rendues anonymes dès qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées. Il est généralement recommandé que les exigences de limitation de conservation des données soient revues périodiquement.

En ce qui concerne la conservation de données à caractère personnel par les autorités publiques aux fins de la lutte contre la criminalité, il convient de faire une distinction en termes de durée de stockage, selon la nature de l'infraction ou selon que la personne concernée est seulement un suspect conformément à l'exigence selon laquelle les données à caractère personnel ne peuvent être traitées que le temps nécessaire à la réalisation de la finalité spécifique.

La coopération au niveau national entre les autorités chargées de la protection des données et les autres autorités de contrôle[49] devrait être facilitée afin que des orientations spécifiques puissent être élaborées pour assurer un équilibre entre les obligations légales applicables, tant du point de vue de la LBC/FT que de la protection des données, y compris sur la question de la conservation des données. Ce type de coopération pourrait être renforcé, par exemple: (i) en organisant des réunions conjointes entre les autorités chargées de la protection des données et d'autres autorités chargées de la protection des données sur la LBC/FT et la protection des données ; (ii) en publiant des lignes directrices communes sur des aspects liés, tels que la technologie nécessaire

49. Cela nonobstant le fait que la législation sur la protection des données mettant en œuvre la Convention 108+, en particulier l'article 15, prévoit les tâches et les pouvoirs des autorités chargées de la protection des données. Toute recommandation concernant la coopération entre les autorités chargées de la protection des données et d'autres autorités chargées de la protection des données (autorités de LBC/FT) devrait être conforme aux tâches et pouvoirs des autorités chargées de la protection des données, et en particulier au rôle de contrôle indépendant des autorités chargées de la protection des données.

(par exemple le niveau de chiffrement ou le calcul multipartite), les ensembles de données nécessaires au traitement pour atteindre les objectifs de LBC/FT, ou comment les personnes concernées devraient pouvoir exercer leurs droits vis-à-vis des responsables du traitement ; (iii) en organisant des consultations avec les autorités chargées de la protection des données[50] dans le cadre de l'élaboration de normes, de lignes directrices et de recommandations, ainsi que la possibilité d'un dialogue informel avec d'autres autorités chargées de la protection des données ; (iv) en invitant les autorités chargées de la protection des données à participer à des réunions informelles sur les PPP, auxquelles des entités du secteur privé ont également la possibilité d'assister en plus des autorités compétentes ; (v) en associant les autorités chargées de la protection des données à l'examen des différents documents d'orientation expliquant comment les institutions financières/EPNFD devraient se conformer à chacune de leurs obligations en matière de LBC/FT, afin de s'assurer que ces documents fournissent suffisamment de détails et d'orientations sur les exigences en matière de protection des données et de la vie privée, et sur la manière dont les entités assujetties peuvent satisfaire aux deux ensembles d'exigences. Cela pourrait également aider à cerner les domaines où il existe une incompatibilité des politiques – qui pourrait ensuite être traitée par un autre forum (par exemple par voie législative).

3.7. Le principe de la sécurité des données

Principe général

La sécurité et la confidentialité des données à caractère personnel sont essentielles pour éviter que la personne concernée ne pâtisse d'événements comme l'accès, l'utilisation, la modification, la divulgation, la perte, la destruction ou l'endommagement des données, que ces événements soient illicites, accidentels ou non autorisés (article 7 de la Convention 108+). Le responsable du traitement et, le cas échéant, le sous-traitant doivent prendre des mesures de sécurité particulières qui tiennent compte de la spécificité des opérations et des méthodes et techniques les plus avancées en matière de sécurité des données. La pertinence des mesures de sécurité doit être déterminée au cas par cas et revu régulièrement.

50. Les autorités chargées de la protection des données sont également régulièrement consultées sur les propositions législatives, y compris dans le cadre d'une consultation publique. La possibilité de consultation est également utilisée au niveau de l'Union européenne : lettres du Comité européen de la protection des données aux institutions européennes sur la protection des données à caractère personnel dans les propositions législatives de LBC-FT, Comité européen de la protection des données (europa.eu).

La «pseudonymisation» est un traitement de données à caractère personnel qui permet que ces dernières ne puissent plus être attribuées à une personne concernée précise sans qu'il soit nécessaire d'avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles garantissant que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. Les mesures de pseudonymisation, qui ne dispensent pas de l'application des principes pertinents de protection des données, peuvent réduire les risques pour les personnes concernées[51].

Étant donné que des problèmes de sécurité des données peuvent survenir dans de nombreuses situations différentes (perte d'intégrité par cyberattaque, perte de confidentialité par interception de transmissions de données, perte de disponibilité, perte de données, black-out, temps d'arrêt), d'autres mesures pourraient également être envisagées ici, telles que l'anonymisation, le chiffrement, les droits d'accès et les rôles, etc.

Dans le contexte de la LBC/FT[52]

Il y a, dans les Recommandations du GAFI, plusieurs exigences adressées aux autorités publiques pour assurer la sécurité des données. La version révisée de la Recommandation 2 demande aux pays une coopération et une coordination entre autorités compétentes afin de garantir la compatibilité des exigences en matière de LBC/FT avec celles concernant la protection des données. Cela aura également un impact (bien que seulement indirect) sur la sécurité des données lorsqu'elles sont traitées et échangées par les entités assujetties.

Garantir la confidentialité des DOS est essentiel à l'efficacité des systèmes de transmission, en évitant que la personne visée de même que des tiers ne soient prévenus, car cela pourrait compromettre la collecte d'informations et porter atteinte aux efforts d'enquête, y compris permettre le déplacement des avoirs. Les règles de confidentialité des DOS sont aussi importantes pour protéger la réputation d'une personne qui ferait l'objet de cette déclaration, ainsi que la sécurité de la personne transmettant la déclaration. À un niveau plus opérationnel, des exigences sont déjà en place pour que les CRF protègent l'information, en particulier : (i) en mettant en place des règles sur la sécurité et la confidentialité des informations, y compris des procédures de gestion, de conservation, de diffusion et de protection, et sur l'accès à cette information ;

51. Lignes directrices du Conseil de l'Europe sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées (2017), voir : https://rm.coe.int/lignes-directrices-sur-la-protection-des-personnes-a-l-egard-du-traite/16806f06d1.
52. Recommandations pertinentes du GAFI : 2, 21, 29, 40.

(ii) en veillant à ce que le personnel ait un niveau de vérification et de compréhension de ses responsabilités lorsqu'il traite et diffuse des informations sensibles et confidentielles ; et (iii) en veillant à limiter l'accès aux locaux et aux systèmes, y compris les technologies de l'information[53]. Outre le GAFI, les Principes d'Egmont stipulent aussi des mesures de sécurité applicables aux échanges d'information. Par ailleurs, des exigences sont prévues pour l'utilisation de canaux sécurisés pour l'échange d'informations applicables aux autorités compétentes comme les cellules d'investigation[54].

Il est possible que la législation sur la protection des données applicables dans les États parties prévoie des exigences détaillées concernant la sécurité des données, lesquelles peuvent être applicables aux entités assujetties en tant que responsables du traitement. Parallèlement, la LBC/FT ou d'autres législations nationales spécifiques peuvent également prévoir des exigences supplémentaires pour garantir la sécurité des données et des informations portées à la connaissance des agents publics des autorités compétentes. Les agents publics peuvent avoir une responsabilité disciplinaire, civile, administrative et pénale en cas de manquement à l'obligation de garantir la sécurité des informations qui sont liées à leurs activités constituant un secret officiel, bancaire, fiscal, commercial ou de communication.

Recommandations

Des exigences spécifiques devraient être imposées aux entités assujetties pour qu'elles appliquent des mesures de sécurité les plus strictes et les plus récentes afin de garantir la protection des données à caractère personnel, en particulier dans le cas de données sensibles (par exemple sur les PPE, qui pourraient révéler des affiliations politiques ou l'orientation sexuelle dans le cas d'un partenariat entre personnes de même sexe), sauf si le cadre applicable en matière de protection des données prévoit déjà de telles exigences directement applicables et donc contraignantes pour les entités assujetties en tant que responsables du traitement.

Le respect du principe de sécurité des données nécessite des mesures techniques et organisationnelles telles que le chiffrement (fort et de bout en bout) des données et des règles de traçabilité complète des échanges, notamment par la mise en place de journaux d'accès, conformément également au principe de responsabilité énoncé dans l'article 10 de la Convention 108+. D'autres garanties devraient également être mises en place, le cas échéant, telles que la pseudonymisation, afin de prévenir toute ingérence illégale dans la vie privée et le droit à la protection des données. Ces mesures techniques

53. GAFI, recommandation 29.
54. GAFI, recommandation 40.

et organisationnelles devraient être fondées sur une évaluation des risques concernant l'impact sur les droits des personnes concernées.

- Les responsables du traitement se doivent d'analyser les menaces et les tendances en matière de cybercriminalité et de sécurité des informations, à la fois régulièrement et de façon ponctuelle (si un événement inattendu le justifie), afin de renforcer la sécurité des données et de réduire le plus possible le risque d'atteinte.

4. Types de données à caractère personnel faisant l'objet d'un traitement dans le cadre des obligations en matière de LBC/FT

Principe général

Comme mentionné ci-dessus, toutes les informations peuvent être des données à caractère personnel à condition qu'elles permettent l'identification d'une personne physique. L'identification n'a pas besoin d'être directe, les informations qui pourraient éventuellement conduire à l'identification d'une personne avec d'autres informations, même si elles ne sont accessibles qu'à distance, constitueraient également des données à caractère personnel.

Parallèlement, il existe des catégories particulières de données à caractère personnel définies à l'article 6 de la Convention 108+ qui exigent que des garanties appropriées soient consacrées par la loi, complétant celles de la convention. Ces données sont : les données génétiques ; les données à caractère personnel concernant des infractions, des procédures pénales et des condamnations et des mesures de sécurité connexes ; les données biométriques identifiant une personne de façon unique ; les données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle, dont le traitement est, par nature, susceptible de présenter un risque plus élevé pour les personnes concernées et doit donc faire l'objet d'une protection accrue. Cela inclut les données dont ces informations ne peuvent être dérivées ou déduites. Ces données sont soumises à des garanties supplémentaires complétant celles déjà en place pour les « données à caractère personnel en général » et ne peuvent être traitées légalement que dans un nombre limité de conditions.

Dans le contexte de la LBC/FT[55]

Afin d'atténuer les risques de LBC/FT, le secteur privé est tenu de prendre des mesures visant la collecte, le traitement et le partage sécurisé des données pertinentes avec les autorités compétentes (par exemple les autorités de surveillance et les services répressifs et de supervision, au niveau national et parfois international, généralement par l'intermédiaire de leurs CRF nationales) et au sein des groupes financiers à des fins de LBC/FT pour la prévention, la détection et le signalement des clients et des opérations qui suscitent un soupçon de BC, d'infraction sous-jacente associée et de FT :

- partager les informations dans le contexte de groupes financiers est requis à la fois à des fins de vigilance à l'égard de la clientèle et de gestion des risques de BC/FT[56] ;
- identifier, évaluer et comprendre la nature et le niveau des risques de BC/FT, et appliquer les politiques, contrôles internes et programmes de LBC/FT nécessaires pour atténuer correctement ces risques[57] ;
- connaître ses clients et appliquer à leurs comptes et à leurs activités un suivi approprié à des fins de LBC/FT[58], en prenant des mesures de vigilance à l'égard de la clientèle pour identifier chaque client et vérifier son identité au moment de l'établissement des relations d'affaires, et en maintenant des mesures de vigilance pendant toute la durée de ces relations ;
- conserver les documents relatifs à la vigilance à l'égard de la clientèle et les autres informations sur les transactions pendant au moins cinq ans[59], étant donné que les enquêtes sur les infractions financières sont souvent très longues ;
- être capable de détecter et de signaler les transactions suspectes[60], et de veiller à ce que les clients ignorent qu'une DOS ou une information s'y rapportant est communiquée aux autorités[61]. Il convient également de reconnaître que certaines catégories particulières de données, notamment celles qui concernent les contributions à des organisations idéologiques/politiques, de paiements d'amendes, etc., sont encore traitées indépendamment de tout contrôle supplémentaire en matière de LBC/FT découlant d'obligations juridiques énoncées dans d'autres cadres internationaux de prévention de la criminalité ;

55. Recommandations pertinentes du GAFI : 1, 10, 11, 18, 20, 21.
56. GAFI, recommandation 18.
57. GAFI, recommandation 1.
58. GAFI, recommandation 10.
59. GAFI, recommandation 11.
60. GAFI, recommandation 20.
61. GAFI, recommandation 21.

- les objectifs de LBC/FTC peuvent conduire au traitement de catégories spéciales de données qui méritent une protection renforcée conformément à l'article 6 de la Convention 108+, mais, actuellement, les données sensibles sont rarement demandées à des fins de LBC/FT. Par exemple, dans les cas où les clients peuvent avoir à s'identifier comme faisant partie d'une relation homosexuelle, l'entité assujettie doit seulement savoir que le client correspond à la définition d'un membre de la famille ou d'un proche associé d'une PPE, sans nécessairement avoir besoin de connaître la nature de la relation.

Différents types de données sont traités dans le domaine de la LBC/FT, et il est important d'en connaître l'étendue. À cette fin, on trouvera en annexe d'autres définitions des types de données et de collectes du point de vue de la LBC/FT.

Recommandations

Les autorités de LBC/FT et de protection des données, dans leurs compétences respectives, veillent à ce que, pour tout traitement de données déterminé, les exigences en matière de LBC/FT et de protection des données soient respectées.

Les entités assujetties ne devraient pas traiter des catégories particulières de données qui ne sont pas directement liées à la finalité poursuivie devant être déterminée à la suite d'une évaluation approfondie de la nécessité et de la proportionnalité du traitement de chaque catégorie de données sensibles[62].

Les données à caractère personnel relatives aux infractions, aux procédures et aux condamnations pénales, ainsi que les mesures de sécurité qui s'y rapportent, font partie des catégories spéciales de données à caractère personnel susmentionnées qui sont également pertinentes pour la lutte contre le blanchiment de capitaux et le financement du terrorisme. Le traitement de ces données ne peut être effectué que s'il est spécifiquement autorisé par la loi et si des garanties appropriées sont en place (par exemple obligation de secret professionnel, mesures faisant suite à une évaluation de l'impact sur la vie privée, mesure de sécurité organisationnelle ou technique particulière et qualifiée, telle que le chiffrement et la journalisation des données[63]).

62. Catégories spéciales de données selon l'article 6 de la Convention 108+: données génétiques; les données à caractère personnel relatives aux infractions, aux procédures pénales et aux condamnations, ainsi qu'aux mesures de sécurité connexes; les données biométriques permettant d'identifier une personne de manière unique; données à caractère personnel pour les informations qu'elles révèlent concernant l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres, la santé ou la vie sexuelle.
63. Voir le rapport explicatif de la Convention 108+, par. 56.

- Les registres avec des informations sur les condamnations pénales devraient être limités aux autorités compétentes, ou au traitement sous le contrôle de ces autorités. Des lignes directrices internes devraient être élaborées pour permettre d'évaluer au cas par cas si la collecte et/ou le transfert de données sensibles (notamment en ce qui concerne la religion et d'autres données sensibles) est nécessaire et proportionné à l'objectif poursuivi, compte tenu des risques possibles pour la vie et l'intégrité des personnes concernées en cas d'incident sur la sécurité des données, y compris une violation des données.

- Les autorités de contrôle devraient édicter des lignes directrices pour le traitement de catégories particulières de données à caractère personnel, y compris sur les mesures appropriées et complémentaires visant à protéger les droits et libertés des personnes concernées, et de prévoir que les décisions de l'entité assujettie et des autorités compétentes ne soient pas fondées uniquement sur ces catégories de données à caractère personnel.

- Toutes les entités impliquées dans la LBC/FT, notamment les entités privées, les CRF et les services répressifs, doivent assurer la formation de leur personnel, en ce qui concerne le traitement des catégories spéciales de données, par exemple concernant la mesure dans laquelle le traitement de ces données est autorisé par la loi.

- En vertu de l'article 10 de la Convention 108+, il est nécessaire que les responsables du traitement rendent compte du traitement appliqué à ce type de données, notamment par des études d'impact sur la protection des données, des mesures prévoyant la confidentialité par défaut et dès la conception, et par la nomination, le cas échéant, d'un délégué à la protection des données.

5. Droits des personnes concernées, exceptions et restrictions dans le contexte de la LBC/FT

Principe général

Les personnes concernées ont de nombreux droits, détaillés dans l'article 9 de la Convention 108+ :

- le droit de ne pas être soumises à une décision les affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que leur point de vue soit pris en compte ;
- le droit d'obtenir, à leur demande, à intervalle raisonnable et sans délai ou frais excessifs, la confirmation d'un traitement de données les concernant, la communication intelligible des données traitées, et toute information disponible sur leur origine, la durée de leur conservation ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements, conformément à l'article 8.1 ;
- le droit d'obtenir, à leur demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement leur sont appliqués ;
- le droit de s'opposer à tout moment, pour des raisons tenant à leur situation, à ce que des données à caractère personnel les concernant fassent l'objet d'un traitement, à moins que le responsable du traitement ne démontre des motifs légitimes justifiant le traitement, qui prévalent sur les intérêts ou les droits et libertés fondamentales des personnes concernées ;
- le droit d'obtenir, à leur demande, sans frais et sans délai excessifs, la rectification de ces données ou, le cas échéant, leur effacement lorsqu'elles sont ou ont été traitées en violation des dispositions de la présente convention ;

- le droit de disposer d'un recours, conformément à l'article 12, lorsque leurs droits prévus par la présente convention ont été violés ;
- le droit de bénéficier, quelle que soit leur nationalité ou leur résidence, de l'assistance d'une autorité de contrôle au sens de l'article 15 pour l'exercice de leurs droits prévus par la présente convention.

Les conditions d'éventuelles restrictions de ces droits sont énoncées à l'article 11 de la Convention 108+ ; elles doivent être prévues par la loi, respecter le contenu essentiel des libertés et des droits fondamentaux, et constituer une mesure nécessaire et proportionnée dans une société démocratique. Les restrictions au droit d'accès ne devraient être levées que lorsque l'accès ne compromet plus les enquêtes.

Les exceptions ne doivent être établies qu'aux fins énumérées à l'article 11 qui comprennent notamment la protection de la sécurité nationale, de la défense, de la sûreté publique et des intérêts économiques et financiers importants de l'État, et ce uniquement en relation avec des droits ou obligations spécifiques énoncés dans l'article.

Dans le contexte de la LBC/FT [64]

Certains des droits énoncés dans la Convention 108+ peuvent être restreints à des fins de LBC/FT. En général, les restrictions fondées sur les lois relatives à la LBC/FT reposent sur l'intérêt public général (c'est-à-dire l'intégrité du système financier ; la prévention, les enquêtes et les poursuites relatives à des infractions pénales, et l'exécution de sanctions pénales). Les droits de la personne concernée sont restreints, par exemple dans une situation où l'entité assujettie signale une transaction suspecte à la CRF. Les lois relatives à la LBC/FT exigent que la déclaration d'opération suspecte ne soit pas divulguée à la personne concernée et permettent ainsi de restreindre son accès aux données à caractère personnel relatives à cette déclaration. D'autres restrictions peuvent être imposées en ce qui concerne le traitement des déclarations d'opération suspecte par la CRF. De même, il n'y a généralement aucune raison de restreindre l'accès aux données relatives à la vigilance à l'égard de la clientèle, et les entités assujetties, conformément à l'article 8 de la Convention 108+, se doivent d'informer les clients que leurs données à caractère personnel peuvent être utilisées à des fins de LBC/FT, y compris lors d'analyses ultérieures, dans le but de faciliter l'exercice des droits des personnes concernées.

64. GAFI, recommandation 21.

Recommandations

Des mesures devraient être mises en place par les responsables du traitement pour faciliter l'exercice de ces droits par la personne concernée, en principe gratuitement. En cas de prise de décision automatisée, et si aucune exception ne s'applique, les informations relatives à la décision doivent être disponibles sur demande de la personne concernée. Le droit de ne pas être soumis uniquement à une prise de décision automatisée devrait également s'appliquer même si l'IA est utilisée pour analyser les données de transaction et pour décider si une transaction est suspecte ou non et si elle devrait être transmise aux services répressifs et de supervision. Des règles et des instructions claires devraient être fournies, conformément à l'article 11, sur la question de savoir si et quand les personnes concernées peuvent exercer leur droit, ou si une exception s'applique et comment la règle de « divulgation »[65] peut être mise en œuvre conformément aux exigences en matière de protection des données.

En ce qui concerne le droit d'opposition, le rapport explicatif (paragraphe 80) indique que, même lorsque ce droit est limité aux fins de la recherche ou de la poursuite d'infractions pénales, la personne concernée peut contester la légalité du traitement. Toute restriction à l'exercice des droits justifiée par le risque de compromettre des enquêtes devrait être levée dès lors que ce risque n'existe plus.

La mise en œuvre effective des droits des personnes concernées peut également nécessiter des actions supplémentaires afin que ces droits s'inscrivent dans une architecture de protection de la vie privée dès la conception, conformément à l'article 10 de la Convention 108+. Par exemple, le droit d'accès peut exiger que l'architecture permette à l'utilisateur d'identifier de manière transparente tous les ensembles de données contenus dans le système, liés aux personnes concernées, et de les choisir sans divulguer les données d'autres personnes (séparation des données ou données structurées intégrées dans l'architecture).

65. GAFI, recommandation 21.*b*.

6. Exceptions et restrictions (article 11)

Principe général

Seules des exceptions aux dispositions de l'article 5.4, de l'article 7.2, de l'article 8.1, et de l'article 9 de la Convention 108+ peuvent être faites, lorsqu'une telle exception est prévue par la loi, respecte l'essence des droits et libertés fondamentaux, et constitue une mesure nécessaire et proportionnée dans une société démocratique.

Le recours à ces exceptions ne peut en aucun cas déroger à l'obligation de veiller à ce que le traitement des données soit effectué par des moyens licites, sur une base juridique appropriée et d'une manière proportionnée à l'objectif poursuivi, compte tenu des intérêts en jeu et de l'incidence sur les droits et libertés individuels.

Il peut être pertinent de noter, en ce qui concerne les activités de traitement à des fins de sécurité et de défense nationales, que, en plus des exceptions spécifiées ci-dessus, des exceptions peuvent être faites à l'article 4.3, à l'article 14.4 et 5, et à l'article 15.2.*a, b, c et d*, à condition qu'elles soient prévues par la loi et qu'elles constituent une mesure nécessaire et proportionnée dans une société démocratique pour satisfaire à la finalité du traitement.

Cela est sans préjudice de l'exigence selon laquelle les activités de traitement à des fins de sécurité et de défense nationales doivent faire l'objet d'un examen et d'une supervision indépendants et efficaces en vertu de la législation nationale de la Partie concernée.

Dans le contexte de la LBC/FT

Sur la base de cette exception, le régime de LBC/FT pourrait prévoir des situations dans lesquelles le client (la personne concernée) n'est pas informé du traitement, en particulier lorsque l'entité assujettie applique une des mesures de vigilance renforcées ou déclare des opérations suspectes. Cela impliquerait une information préalable du client, ce qui contreviendrait aux

interdictions de LBC/FT, en particulier aux exigences en matière de divulgation. Par ailleurs, toute exception au droit d'accès des clients devrait être utilisée par les autorités compétentes dans la mesure où, et aussi longtemps qu'une telle mesure satisfait aux conditions énoncées à l'article 11 de la Convention 108+ (par exemple une mesure prévue par la loi, qui respecte l'essence des droits et libertés fondamentaux, et qui constitue une mesure nécessaire et proportionnée dans une société démocratique).

Recommandations

- Lorsque les droits des personnes concernées sont restreints à des fins de LBC/FT, ces restrictions devraient reposer sur la législation en matière de LBC/FT, respecter l'essence des droits et libertés fondamentaux et se limiter strictement à ce qui est nécessaire et proportionné dans une société démocratique. Elles ne devraient en aucun cas être trop larges ou servir d'autorisation générale, et ne devraient s'appliquer qu'aux domaines couverts par l'article 11.1 de la Convention 108+.

- Toute restriction à l'exercice des droits justifiée par le risque de compromettre des enquêtes devrait être levée dès lors que ce risque n'existe plus.

7. Le rôle des autorités de protection des données et leur relation avec les autorités de la LBC/FT

Principe général

Dans le contexte de la protection des données, les autorités chargées de la protection des données sont des organismes publics ayant la mission, assortie des pouvoirs nécessaires, d'assurer la conformité avec la réglementation applicable en matière de protection des données, notamment par des mesures répressives et une coopération internationale.

Selon l'article 15, aux termes de la Convention 108+, les autorités de contrôle ont notamment des pouvoirs d'enquête et d'intervention, exercent des fonctions relatives aux transferts de données, ont le pouvoir de prendre des décisions en cas de violation des dispositions de la convention et d'imposer des sanctions.

Les articles 16 et 17 de la Convention 108+ prévoient des moyens de coopération et d'assistance mutuelle entre les autorités de contrôle de la protection des données.

Dans le contexte de la LBC/FT

Les activités nécessaires pour se conformer à la réglementation en matière de LBC/FT impliquent l'activité de différents acteurs parfois dans de multiples juridictions ainsi que le traitement de vastes volumes de données à caractère personnel. La Convention 108+ prévoit que les pouvoirs des autorités de contrôle, notamment en ce qui concerne les enquêtes, les interventions, l'autorisation, le blocage du flux transfrontière de données à

caractère personnel, s'appliquent au traitement de données à des fins de LBC/FT. Bien qu'aucune restriction ne puisse être apportée à l'utilisation de ces pouvoirs lors du traitement des données dans le cadre du maintien de l'ordre (et d'autres objectifs généraux d'intérêt public), l'article 11.3 prévoit, en ce qui concerne les activités de traitement à des fins de sécurité nationale et de défense, que certains de ces pouvoirs peuvent être restreints, à condition que cette restriction soit prévue par la loi, respecte l'essence des libertés et droits fondamentaux et constitue une mesure nécessaire et proportionnée dans une société démocratique. Même dans ce dernier cas, la Convention 108+ exige que les activités de traitement à des fins de sécurité nationale et de défense fassent l'objet d'un contrôle et d'une supervision indépendants effectifs en vertu de la législation nationale de la Partie concernée.

Recommandations

- Les traitements pour la LBC/FT doivent faire l'objet d'une autorisation ou d'un examen *ex-ante* et/ou *ex-post* effectif, cohérent et indépendant, fondé sur le cadre juridique national conformément à l'article 11.3 de la Convention 108+. Cela peut inclure que les cadres juridiques nationaux prévoient un niveau spécifique d'habilitation de sécurité pour le personnel des autorités chargées de la protection des données afin qu'il accède aux données traitées par les CRF relevant de la catégorie des services de renseignement.

- Les autorités chargées de la protection des données doivent coopérer avec les autres autorités nationales chargées de la LBC/FT, afin de mener des activités conjointes pour assurer la conformité avec les normes de protection des données dans le cadre de la répression.

- En général, la nécessité d'un dialogue et d'une coopération entre les autorités de protection des données et d'autres autorités compétentes en matière de LBC/FT (éventuellement aux niveaux national et international) devrait être soulignée afin de développer des outils d'orientation efficaces et des modes opératoires en matière de conformité en élaborant des orientations pratiques tant pour le secteur public que pour le secteur privé, et d'élaborer, le cas échéant, des modules de formation spécifiques.

8. Transferts internationaux de données dans le domaine de la LBC/FT

Principe général

Les flux transfrontières de données se produisent lorsque des données à caractère personnel sont divulguées ou mises à la disposition d'un destinataire qui relève de la juridiction d'un autre État ou d'une autre organisation internationale[66].

Les données à caractère personnel circulent librement entre les Parties à la Convention 108+. Des restrictions à la libre circulation transfrontière des données à caractère personnel sont prévues lorsque : (i) il existe un risque réel et sérieux que la communication à une autre Partie entraîne le contournement des dispositions de la convention ; ou (ii) lorsque des Parties sont liées par des règles de protection harmonisées partagées par des États appartenant à une organisation internationale régionale (article 14.1 de la Convention 108+).

Les transferts de données à caractère personnel à des pays tiers ou à des organisations internationales ne sont possibles que si un niveau approprié de protection peut être garanti, soit par la législation du pays ou de l'organisation destinataire, soit par des garanties ad hoc ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables, adoptés par les personnes impliquées dans le transfert et le traitement ultérieur des données (article 14, alinéas 2 et 3, de la Convention 108+).

Dans des situations spécifiques de transfert de données à caractère personnel vers des territoires où les données ne sont pas correctement protégées, certaines dérogations sont prévues, à condition qu'elles respectent les

66. Rapport explicatif de la Convention 108+, paragraphe 102.

principes de nécessité et de proportionnalité, aux conditions suivantes : (i) la personne concernée a donné son consentement ; (ii) des intérêts spécifiques de la personne concernée nécessitent un tel transfert dans un cas particulier ; (iii) des intérêts légitimes prépondérants, notamment des intérêts publics importants, sont prévus par la loi et le transfert constitue une mesure nécessaire et proportionnée dans une société démocratique ; (iv) le transfert constitue une mesure nécessaire et proportionnée dans une société démocratique pour la liberté d'expression (article 14.4 de la Convention 108+).

Dans le contexte de la LBC/FT[67]

Compte tenu de la nature multilatérale des mécanismes d'échanges interétatiques de données à caractère personnel à des fins de LBC/FT, la question du niveau approprié de protection se pose dans tous les cas où l'échange de telles données concerne un pays qui ne dispose pas d'un niveau (essentiellement) équivalent de protection des données à caractère personnel.

Il y a dans les recommandations du GAFI adressées aux autorités publiques plusieurs exigences en matière de sécurité des données, qui s'appliquent lorsque les données franchissent les frontières. À titre d'illustration, la recommandation 2 du GAFI exige des pays une coopération et une coordination entre les autorités de protection des données et LBC/FT pour veiller à ce que les principes, règles et considérations en matière de protection des données soient dûment intégrés dans les obligations en matière de LBC/FT.

Le GAFI[68] demande aux autorités compétentes, indépendamment des voies et moyens de la coopération internationale, de garder confidentielles les demandes de coopération et les informations échangées, conformément aux obligations des deux parties en matière de protection des données et de la vie privée. Les autorités compétentes sont tenues, au minimum, de protéger les informations échangées de la même façon qu'elles protègent les informations similaires reçues de sources nationales. Les autorités compétentes devraient avoir la possibilité de refuser de fournir des informations si l'autorité compétente requérante n'est pas en mesure de protéger efficacement ces dernières.

Le partage d'informations sur un client entre entités assujetties appartenant au même groupe (données relatives à l'obligation de vigilance à l'égard du client, données indiquant que ce client a fait l'objet d'une DOS, etc.) est généralement considéré comme moins délicat si des exigences et politiques claires précisent quelles informations peuvent être partagées et à quelles fins spécifiques, et si l'échange se produit entre entités assujetties situées

67. GAFI, recommandations pertinentes : 2, 18, 40.
68. GAFI, recommandation 18.

dans le même pays (et donc soumises aux mêmes exigences). Cependant, il se peut que des entités assujetties appartenant au même groupe opèrent depuis différents pays aux exigences variables (voir les considérations sur les flux transfrontières).

Recommandations

- Les entités assujetties devraient, conformément à l'article 14 de la Convention 108+, évaluer l'impact potentiel des transferts prévus et/ou d'autres activités de traitement de données sur les droits et les libertés fondamentaux des personnes concernées avant d'entamer un traitement, et devrait concevoir le traitement des données de manière à prévenir ou à minimiser le risque d'atteinte à ces droits et libertés fondamentaux (article 10.2 de la Convention 108+). Si aucune exception prévue à l'article 14.4 ne s'applique, une telle évaluation du pays ou de l'organisation de destination devrait viser à garantir que le niveau de protection offert par la Convention 108+ est garanti par les destinataires et que la personne concernée est en mesure de défendre ses intérêts, en cas de non-conformité. Les entités assujetties devraient également tenir compte de la force exécutoire des droits des personnes concernées et de la mise à disposition de recours administratifs et judiciaires efficaces pour les personnes concernées dont les données à caractère personnel sont transférées.

- Il est nécessaire d'assurer la collaboration entre autorités de protection des données, pouvoirs publics et organisations internationales en vue d'intégrer les règles et recommandations relatives à la protection des données aux normes internationales de LBC/FT, afin de faciliter les flux transfrontières de données et une mise en œuvre cohérente.

- Les autorités chargées de la protection des données jouent un rôle important, conformément à l'article 15.2.*b* de la Convention 108+, pour garantir la licéité du traitement, même dans un contexte de flux transfrontière de données, y compris le cas échéant, en renvoyant les cas individuels de transferts transfrontières de données devant les tribunaux nationaux. Les autorités chargées de la protection des données doivent avoir le pouvoir, les ressources et accords institutionnels nationaux et internationaux en place pour traiter ces questions en vertu de l'article susmentionné et des exceptions prévues à l'article 11.

- Les autorités chargées de la protection des données doivent être dotées des ressources nécessaires à l'exercice efficace de leurs fonctions et à l'exercice de leurs pouvoirs, y compris en ce qui concerne la mise en œuvre des règles relatives aux flux transfrontières de données à caractère personnel.

Les transferts internationaux de données ne sont autorisés que dans les limites géographiques des pays qui offrent un niveau de protection adéquat ou des garanties appropriées qui sont en place en ce qui concerne le transfert en cause et qui lient l'entité destinataire[69], et en supposant que les autres exigences de la Convention 108+ pour le traitement de ces données soient respectées. Cela s'applique à tout projet ou plans conjoints tels que la mise en commun de données entre institutions financières, notamment au-delà des frontières nationales et avec des non-Parties.

Les États devraient veiller à ce que, lorsque des transferts de données ont lieu vers un pays qui n'assure pas un niveau approprié de protection, les garanties prévues par le cadre international de protection des données, et en particulier par la Convention 108+, soient respectées, notamment à travers des instruments qui garantissent un niveau approprié de protection, conformément à l'article 14.2 ou qui satisfont aux exigences de l'article 14.4.

Dans le cas d'une entité assujettie appartenant à un groupe composé de différentes entités juridiques/filiales situées dans différents pays, lorsque la législation nationale n'interdit pas les transferts transfrontières de données, y compris pour des motifs de protection des données, de tels transferts reposeront sur des garanties standardisées ad hoc ou approuvées. Le transfert ne doit pas porter atteinte au niveau approprié de protection des données à caractère personnel.

Les CRF des États parties devraient échanger des informations avec d'autres autorités compétentes et avec leurs homologues étrangers conformément aux exigences applicables, et limiter les données à caractère personnel traitées à ce qui est directement pertinent pour fournir ou obtenir les informations demandées. En ce qui concerne les transferts de données à caractère personnel vers des États non parties à la Convention 108+, les exigences prévues à l'article 14 de la Convention 108+ doivent être respectées. Des normes additionnelles applicables à l'échange d'informations pourraient s'appliquer et préciser les exigences en matière de protection ou de sécurité des données[70]. Il convient de noter que le deuxième protocole additionnel à la Convention de Budapest (STE n° 185) et ses protocoles pourraient donner des indications supplémentaires sur les garanties applicables en matière de transferts internationaux entre autorités et, dans une certaine mesure, entre autorités et parties privées.

69. Article 14.4 de la Convention 108+ et par. 109 à 112 du rapport explicatif.
70. Telles que les principes du Groupe Egmont.

- Les États parties devraient veiller à ce que les dérogations à l'exigence d'un niveau approprié de protection des données ne soient autorisées que lorsque les conditions énoncées à l'article 14.4 sont remplies.

- Il serait utile d'envisager d'intégrer directement les règles et considérations relatives à la protection des données dans les recommandations du GAFI, afin de faciliter l'harmonisation de leur mise en œuvre respective.

- La coopération entre les autorités chargées de la protection des données et d'autres autorités compétentes en matière de LBC/FT est à recommander, tant au niveau interne concernant les exportations de données qu'au niveau multilatéral pour faciliter les transferts de données à caractère personnel avec un niveau de protection approprié.

Annexe

Données clients : les normes du GAFI définissent des paramètres pour le partage d'informations uniquement dans le contexte d'un groupe financier[71]. En raison des exigences en matière de protection des données et de confidentialité, le partage de données en dehors d'un groupe financier est limité. Les ensembles de données relatives aux mesures de vigilance à l'égard de la clientèle qui doivent être obtenus auprès d'une personne physique comprennent principalement des données à caractère personnel, telles que: le nom complet, l'adresse résidentielle, le numéro de contact et les adresses électroniques, le lieu de naissance, la date de naissance, le sexe, la nationalité, le numéro d'identification délivré par le gouvernement et le numéro d'identification fiscale, la signature. Pour une personne morale ou une construction juridique, certaines données à caractère personnel sont également requises sur les administrateurs, les actionnaires, les hauts responsables et les bénéficiaires effectifs, qui sont généralement accessibles au public en raison de dispositions légales fondées sur l'intérêt public[72].

Informations sur les bénéficiaires effectifs : d'après la définition du GAFI, le bénéficiaire effectif est toujours une ou plusieurs personnes physiques qui, en dernier lieu, possèdent ou contrôlent un client, une personne morale ou une construction juridique, et/ou la personne physique pour le compte de laquelle une opération est effectuée. Dans ce contexte, les jeux de données comportent principalement l'identification du bénéficiaire effectif et ses coordonnées de contact (nom complet, nationalité(s), lieu et date de naissance détaillés, adresse du domicile, numéro d'identification national et type de document, numéro d'identification fiscale ou équivalent dans le pays de résidence) et des informations sur le patrimoine immobilier, l'origine du patrimoine et des fonds, l'activité professionnelle et le fait que le bénéficiaire

71. Selon la définition du glossaire du GAFI, un groupe financier constitue « un groupe constitué d'une société mère ou de tout autre type de personne morale exerçant des fonctions de contrôle et de coordination sur le reste du groupe ainsi que des succursales et/ou des filiales soumises aux politiques et procédures de LBC/FT au niveau du groupe ».
72. Toutefois, les exigences du GAFI exigent seulement que la liste des administrateurs soit accessible au public. Le reste ne doit être accessible qu'aux autorités compétentes.

effectif soit ou non une PPE. Les données d'identification pertinentes peuvent être obtenues à partir des registres publics ou auprès du client ou d'autres sources fiables. Pour être jugées suffisantes, les informations doivent permettre l'identification de la personne physique qui est bénéficiaire effectif et des moyens et mécanismes par lesquels son contrôle s'exerce. Pour être exactes, les informations doivent être vérifiées à l'aide de sources/de l'obtention de documents, données ou informations fiables et indépendantes, dans la mesure de ce qui est nécessaire au regard du niveau de risque spécifique. Les informations doivent être actuelles et mises à jour dans un délai raisonnable lors de chaque changement.

Personnes politiquement exposées (PPE) : elles sont classées, selon les normes du GAFI, dans trois catégories principales, comme décrit ci-dessous. La définition des PPE ne vise pas les personnes de rang intermédiaire ou plus subalterne dans les catégories précédentes. Par ailleurs, la collecte de données sur des PPE peut révéler les affiliations politiques ou l'orientation sexuelle (dans le cas, par exemple, d'un partenariat avec une personne de même sexe). Par conséquent, le traitement de ces catégories de données à caractère personnel ne pourrait être licite que s'il bénéficie d'une protection renforcée.

- Les **PPE étrangers**, qui sont des personnes qui sont ou ont été chargées de fonctions publiques importantes par un pays étranger, par exemple des chefs d'État ou de gouvernement, des hauts responsables politiques, des hauts fonctionnaires, des fonctionnaires judiciaires ou militaires, des cadres supérieurs de sociétés d'État, des responsables importants de partis politiques.
- Les **PPE nationaux**, qui sont des personnes qui sont ou ont été chargées au niveau national de fonctions publiques importantes, par exemple des chefs d'État ou de gouvernement, des hauts responsables politiques, des hauts fonctionnaires, des fonctionnaires judiciaires ou militaires, des cadres supérieurs d'entreprises publiques, des responsables importants de partis politiques.
- Les **personnes qui sont ou ont été chargées d'une fonction importante par une organisation internationale** désignent les membres de la haute direction, c'est-à-dire les administrateurs, les directeurs adjoints et les membres du conseil d'administration ou des fonctions équivalentes.

Les données financières peuvent englober les informations sur les comptes (coordonnées bancaires et finalités du compte) et sur les opérations (historiques des opérations, des crédits, des cartes et de leur utilisation ; adresse IP ; retraits en distributeurs automatiques ; informations sur la clôture de comptes ou l'interruption des relations d'affaires en raison de soupçons ; analyses menées sur un schéma de transactions dans le contexte du profil

financier). Ces données comptent parmi les plus sensibles, puisqu'elles révèlent la situation financière de l'intéressé, ses interactions familiales, ses habitudes et comportements, l'état de son patrimoine, etc.[73]

Statistiques : la recommandation 33 du GAFI demande aux pays de tenir des statistiques complètes sur les questions relatives à l'effectivité et à l'efficacité de leur système de LBC/FT, qui devraient comprendre des statistiques sur : (i) les DOS reçues et diffusées ; (ii) les enquêtes, poursuites et condamnations relatives au BC/FT ; (iii) les biens gelés, saisis ou confisqués et (iv) l'entraide judiciaire et les autres demandes internationales de coopération. L'une des principales difficultés identifiées tient à l'absence, au niveau international, de consensus et d'orientations sur les types de données spécifiques qui devraient être collectées[74].

En vertu de la recommandation 24 du GAFI, le **traitement de données** est requis pour les « actionnaires ou administrateurs désignés », et peut inclure les données à caractère personnel. Un actionnaire désigné (*nominee shareholder*) est un individu ou une personne morale qui agit, à un certain titre, au nom et sous réserve des instructions d'un autre individu ou d'une personne morale (« le désignateur[75] ») à l'égard d'une personne morale. Un administrateur désigné (*nominee director*) est un individu ou une personne morale qui exerce au quotidien des fonctions d'administration dans une entreprise pour le compte du désignateur et en suivant ses instructions, directes ou indirectes. Un administrateur désigné (directeur ou actionnaire) n'est jamais le bénéficiaire effectif d'une personne morale.

Conformément à la recommandation 25 du GAFI, le **traitement de données**, y compris à caractère personnel, est nécessaire pour les trusts et les autres constructions juridiques. Ces données comprennent l'identité du constituant, du ou des administrateurs ou *trustees*, du protecteur (le cas échéant), des bénéficiaires ou de la catégorie de bénéficiaires et de toute autre personne physique exerçant en dernier lieu un contrôle effectif sur le trust, y compris au travers d'une chaîne de contrôle ou de propriété. Les termes « trust » et « *trustee* » sont à comprendre au sens de l'article 2 de la Convention de La Haye relative à la loi applicable au trust et à sa reconnaissance. Les *trustees* peuvent

73. Rapport du GAFI, « Stocktake on data pooling, collaborative analytics and data protection », juillet 2021, page 27.
74. GAFI, Guidance on AML/CFT – related data and statistics (en anglais uniquement, page 10).
75. Par désignateur (*nominator*), on entend un individu (ou groupe d'individus) ou une personne morale qui adresse (directement ou indirectement) des instructions à une personne désignée pour qu'elle agisse pour son compte en qualité d'administrateur ou d'actionnaire ; on parle parfois de « commanditaire » (*silent partner*) ou d'« administrateur de fait » (*shadow director*).

être professionnels (avocats ou sociétés de fiducie par exemple, selon les territoires) s'ils sont rémunérés pour agir en cette qualité dans le cadre de leurs activités commerciales, ou non professionnels (si, par exemple, ils opèrent sans rétribution pour le compte d'une famille).

Les autorités publiques doivent indiquer que la conservation des données a pour but de lutter contre la criminalité. À cet égard, une recommandation antérieure a confirmé la nécessité d'établir une distinction en fonction de la nature ou du degré de gravité de l'infraction ou selon que la personne concernée est seulement un suspect.

Personne morale : selon le glossaire du GAFI, l'expression « personne morale » désigne toute entité autre qu'une personne physique pouvant établir une relation d'affaires permanente avec une institution financière ou détenir des biens de toute autre manière. Sont compris dans cette notion les sociétés, les fondations, les instituts, les sociétés de personnes, les associations et toute autre entité similaire.

Constructions juridiques : selon le glossaire du GAFI, l'expression « constructions juridiques » désigne les trusts exprès ou les constructions juridiques similaires. Des exemples de constructions similaires (aux fins de LBC/FT) sont le trust, le *Treuhand* ou le *Fideicomiso* et le *waqf*.

Le blanchiment de capitaux et le financement du terrorisme sont des phénomènes criminels impliquant des stratagèmes transfrontières et l'utilisation abusive d'institutions financières et non financières dans plusieurs juridictions. Le partage de données entre acteurs étatiques et non étatiques est crucial pour lutter efficacement contre ces phénomènes. Le traitement des données à caractère personnel à ces fins peut constituer une ingérence dans le droit de la personne concernée au respect de la vie privée, tel que protégé par l'article 8 de la Convention européenne des droits de l'homme et d'autres instruments internationaux relatifs aux droits de l'homme.

La lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) vise à prévenir, enquêter et poursuivre ces crimes, par des mesures mises en œuvre par de multiples acteurs. La Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme est ainsi l'une des normes internationales les plus appréciées et les plus largement utilisées à ces fins.

L'objectif des lignes directrices est de fournir une orientation sur la manière d'intégrer les dispositions de la Convention modernisée du Conseil de l'Europe sur la protection des données (Convention 108+) dans la LBC/FT pour fournir un niveau approprié de protection des données tout en facilitant les flux transfrontières de données, et de mettre en évidence certains domaines dans le contexte de la LBC/FT où les garanties de protection des données doivent être renforcées.

PREMS 109923

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE